

datamax+

HSPA 4-Port Ethernet Router with RS232, Wi-Fi & GPS | MA100-1010

CHOOSE WELL...
CHOOSE WISELY...
CHOOSE MAXON...

Datamax+ (MA100-1010) HSPA 4-Port Ethernet Router with GPS, RS232 & Wi-Fi User Manual



 **maxon**
australia.
www.maxon.com.au

This document is the sole and exclusive property of Maxon Australia.
Not to be distributed or divulged without prior written agreement.

170908



TABLE OF CONTENTS

CONTACT INFORMATION	3
RF EXPOSURE COMPLIANCE	4
Caution	4
REVISION HISTORY	7
1. Introduction.....	8
1.1. Specifications	10
2. Installation Introduction.....	14
2.1. General.....	14
2.2. Package Contents	14
2.3. Installation and Cable Connection	14
2.4. Accessories List	15
2.5. SIM card Installation	15
2.6. Antenna Installation.....	15
2.7. Power	16
2.8. Indicator Lights Introduction	16
2.9. Reset Button.....	17
3. Configuration and Management	18
3.1. Management and configuration	21
3.1.1. Setting	21
3.1.2. Wireless.....	40
3.1.3. Services.....	53
3.1.4. VPN.....	61
3.1.5. Security	74
3.1.6. Access Restrictions	78
3.1.7. NAT.....	81
3.1.8. QoS Setting.....	84
3.1.9. Applications.....	86
3.1.10. Administration	88
3.1.11. Status	94
4. Chapter 4 Appendix.....	107

CONTACT INFORMATION

In keeping with Maxon's dedicated customer support policy, we encourage you to contact us.

TECHNICAL:

Hours of Operation: Monday to Friday 8.30am to 5.30pm*

Telephone: +61 2 8707 3000

Facsimile: +61 2 8707 3001

Email: support@maxon.com.au

* Public holidays excluded

SALES:

Hours of Operation: Monday to Friday 8.30am to 5.30pm*

Telephone: +61 2 8707 3000

Facsimile: +61 2 8707 3001

Email: sales@maxon.com.au

* Public holidays excluded

WEBSITE: www.maxon.com.au

Maxon has also added for the benefit of developers and integrators, a forum on our website that can be accessed to discuss this product and/or technical matters in relation to your applications. All questions raised within this portal will be answered.

FORUM: www.maxon.com.au/forum

ADDRESS:

Maxon Australia Pty Ltd
36a Gibson Avenue, Padstow
Sydney, NSW, Australia 2211

POSTAL ADDRESS

Maxon Australia Pty Ltd
Po Box 1, Revesby North,
Sydney, NSW Australia 2212

RF EXPOSURE COMPLIANCE

The use of this device in any other type of host configuration may not comply with the RF exposure requirements and should be avoided. During operation, a 20 cm separation distance should be maintained between the antenna, whether extended or retracted, and the user's/bystander's body (excluding hands, wrists, feet, and ankles) to ensure RF exposure compliance.

Caution

Change or modification without the express consent of Maxon Electronics Australia Pty. Ltd. voids the user's authority to use the equipment. These limits are designed to provide reasonable protection against harmful interference in an appropriate installation. The modem is a transmitting device with similar output power to a mobile phone. This equipment generates, uses, and can radiate radio frequency energy and, if not used in accordance with instructions, can cause harmful radiation to radio communication. The modem is approved for use with the antenna: ANT-8530. Unauthorized antennas, modifications, or attachments could impair call quality, damage the device, or result in violation of RF exposure regulations.

However, there is no guarantee that interference will not occur in a particular installation. If the equipment does cause harmful interference in radio and television reception, which can be determined by turning the equipment on and off, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-orient or relocate the receiving radio or TV antenna
- Increase the separation distance between the equipment and the receiver
- Contact Maxon Australia Technical Support for assistance.

Notes The user is cautioned that changes or modifications not expressly approved by Maxon Australia could void the warranty.



* The product needs to be supplied by a limited power source or the power supply provided. Otherwise, safety will not be ensured

Potentially Unsafe Areas

Posted Facilities: Turn off this device in any facility or area when posted notices require you to do so.

Blasting Areas: Turn off your device where blasting is in progress. Observe restrictions and follow any regulations or rules.

Potentially Explosive Atmospheres: Turn off your device when you are in any area with a potentially explosive atmosphere. Obey all signs and instructions. Sparks in such areas could cause an explosion or fire, resulting in bodily injury or death.

Areas with a potentially explosive atmosphere are often but not always clearly marked. They include:

- fuelling areas such as gas or petrol stations
- below deck on boats
- transfer or storage facilities for fuel or chemicals
- vehicles using liquefied petroleum gas, such as propane or butane
- areas when the air contains chemicals or particles such as grain, dust or metal powders
- avoid using the modem in areas that emit electromagnetic waves or enclosed metallic structures e.g. lifts or any other area where you would normally be advised to turn off your engine

REVISION HISTORY

Product	Datamax+ HSPA Ethernet Router with RS232 & wifi.
Model	MA100-1010
Document Type	PDF
Current Version Number	1.1
Status of the Document	Public Release
Revision Date	May 2014
Total Number of Pages	109

– Revision History

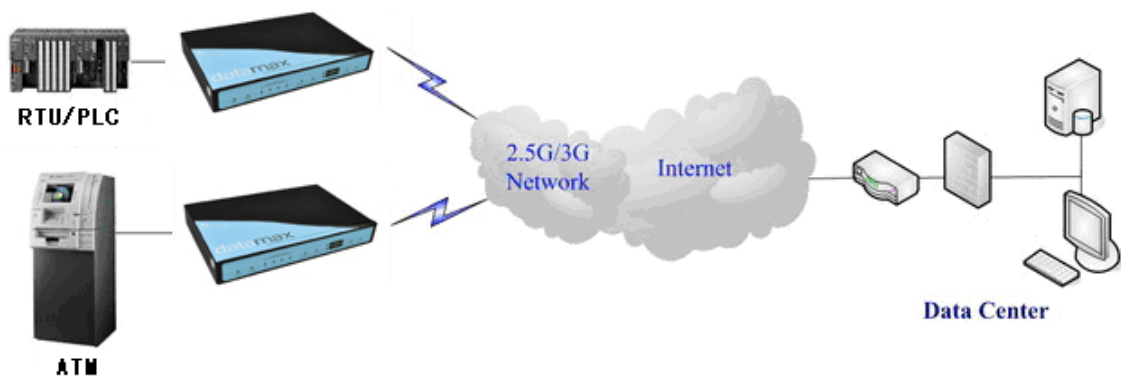
Level	Date	History
1.0	July 2013	Release Version
1.1	May 2014	Minor updates
1.2	Jan 2015	Removed reference to RS422/RS485

1. Introduction

MA100-1010 is a HSPA+ Ethernet router providing data communications via the public cellular network.

The MA100-1010 utilises an industrial 32-bit CPU embedded with an embedded operating system. The device supports RS232 connection, four Ethernet ports and Wi-Fi that conveniently and transparently connect one device to a cellular network, allowing you to connect to your existing serial and Ethernet devices with minimal configuration.

The MA100-1010 has been widely used within M2M applications, such as intelligent transportation, smart grid, industrial automation and telemetry.



Features and Benefits

Designed for Industrial Application

- Industrial cellular module EM820W
- High-powered industrial 32bit CPU
- Industrial GPS module
- Supports low power consumption mode, including sleep mode.
- Metal housing.
- Voltage range: 5~35VDC
- Auto recovery functionality, including online detection, and auto redial.
- Ethernet port: 1.5KV magnetic isolation protection
- RS232: 15KV ESD protection

- SIM port: 15KV ESD protection
- Power port 2.5mm Barrel connector: reverse-voltage and overvoltage protection
- Antenna port SMA Female
- Supports IP Stack Auto mode
- IP / web based user interface for remote management, maintenance and configuration.

Standard and Convenience

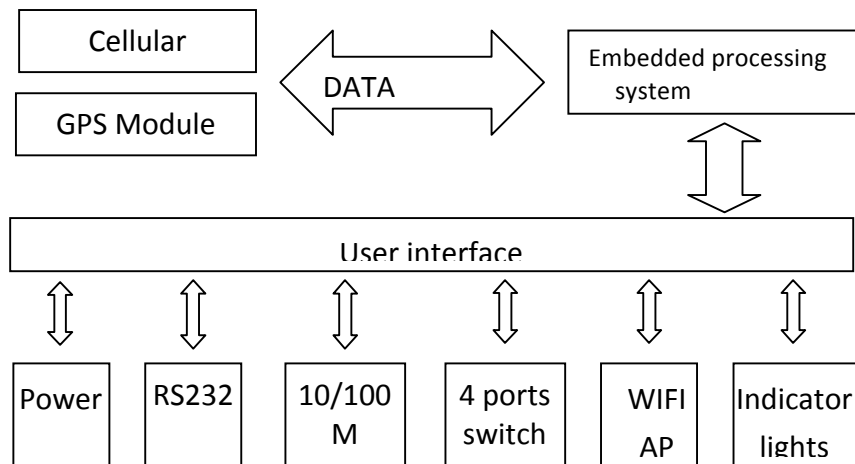
- Supports standard RS232, Ethernet ports and Wi-Fi.
- Supports standard WAN port and PPPOE protocol that can connect to ADSL directly
- Supports intellectual mode, establishes communication state automatically when powered on
- Provide management software for remote management
- Convenient configuration and maintenance interface (WEB or CLI)

High-performance

- Supports multiple WAN access methods, including static IP, DHCP, L2TP, PPTP, PPPOE, 3G/HSPA/4G.
- Supports GPS function
- Supports double link backup between 3G and WAN(PPPOE, ADSL)
- Supports VPN client(PPTP, L2TP, OPENVPN, IPSEC and GRE)
- Supports VPN server(PPTP, L2TP, OPENVPN, IPSEC and GRE)
- Supports local and remote firmware upgrade, import and export config file.
- Supports NTP, RTC embedded.
- Supports multiple DDNS provider service.
- Supports VLANs, MAC Address clone, PPPoE Server
- WIFI support 802.11b/g/n. support AP, client, Adhoc, Repeater, and Bridge.
- WIFI support WEP, WPA, WPA2 encryption, Support RADIUS authentication and MAC address filter.
- Support DHCP server and client, firewall, NAT, DMZ host , URL block, QoS, ttraff, statistics, real time link speed statistics etc.
- Full protocol support, such as TCP/IP, UDP, ICMP, SMTP, HTTP, POP3,

OICQ, TELNET, FTP), SNMP, SSHD, etc.

- Schedule Reboot, Schedule Online and Offline.
- Router chart is as follows



1.1. Specifications

Cellular Specification

Standard and Band	Bandwidth	TX power	RX sensitivity
DATAMAX+ GPS+WCDMA WIFI ROUTER			
UMTS/WCDMA/HSDPA/HSUPA /HSPA+ 850/1900/2100MHz 850/900/1900/2100MHz(optional) GSM850/900/1800/1900MHz GPRS/EDGE CLASS 12	HSUPA:5.76Mbps (Upload speed) HSDPA:7.2Mbps (Download speed) UMTS:384Kbps (DL/UL) HSPA+: 21 Mbps (Download speed) 5.76Mbps (Upload speed)	<24dBm	<-109 dBm

GPS Specification

Item	Content
GPS Module	Industrial GPS module
Receiver Type	50-channle GPS L1 (1575.42MHz) C/A code SBAS: WAAS,EGNOS,MSAS,GAGAN Support GALILEO
Max. update rate	4 Hz
Accuracy	Position: 2.5m CPE SBAS: 2.0m CPE

Acquisition	Cold starts: 29S Warm starts: 29S Aided starts: <1S Hot starts: <1S
Sensitivity	Tracking: -160dBm Reacquisition: -160dBm Cold starts: -144dBm
Timing accuracy	RMS: 30ns 99%: <60ns Granularity: 21ns
Time pulse	Configurable, 0.25 to 1000Hz

WIFI Specification

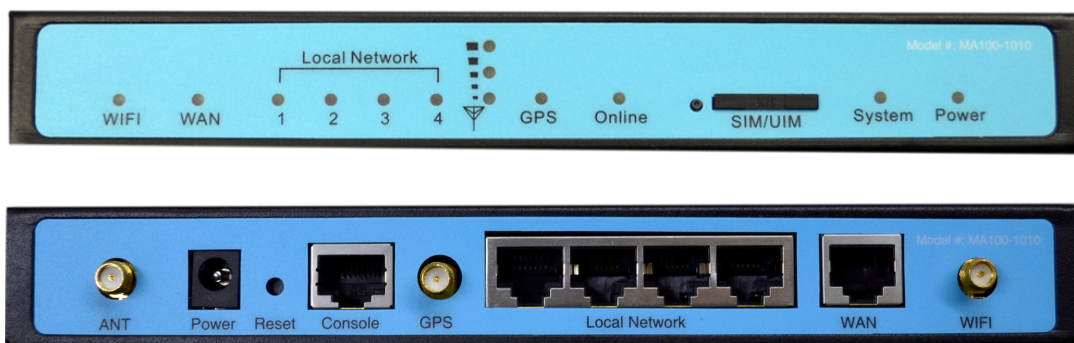
Item	Content
Standard	IEEE802.11b/g/n
Bandwidth	IEEE802.11b/g: 54Mbps (max) IEEE802.11n: 150Mbps (max)
Security	WEP, WPA, WPA2, etc. WPS (optional)
TX power	21.5dBm (11g) , 26dBm (11b)
RX sensitivity	<-72dBm@54Mbps

Hardware System

Item	Content
CPU	Industrial 32bits CPU
FLASH	8MB(Extendable to 64MB)
SDRAM	64MB

Interface Type

Item	Content
WAN	1 10/100 Mbps WAN port(RJ45), auto MDI/MDIX, 1.5KV magnetic isolation protection
LAN	4 10/100 Mbps Ethernet ports(RJ45), auto MDI/MDIX, 1.5KV magnetic isolation protection
Serial	1 RS232 port, 15KV ESD protection Data bits: 5, 6, 7, 8 Stop bits: 1, 1.5(optional), 2 Parity: none, even, odd, space(optional), mark(optional) Baud rate: 2400~115200 bps
Indicator	"Power", "System", "Online", "GPS", " Local Network ", "WAN", "WIFI", "Signal Strength"
Antenna	Cellular: Standard SMA female interface, 50 ohm WIFI: Standard SMA male interface, 50 ohm GPS: standard SMA female interfaces
SIM/UIM	Standard 3V/1.8V user card interface, 15KV ESD protection
Power	Standard 3-PIN power jack, reverse-voltage and overvoltage protection
Reset	Restore the router to its original factory default settings



Power Input

Item	Content
Standard Power	DC 12V/1.5A
Power Range	DC 5~35V
Consumption	<650mA (12V)

Physical Characteristics

Item	Content
Housing	Iron, providing IP30 protection
Dimensions	206x135x28 mm
Weight	790g

Environmental Limits

Item	Content
Operating Temperature	-35~+75°C (-31~+167°F)
Storage Temperature	-40~+85°C (-40~+185°F)
Operating Humidity	95% (Non-condensing)

2. Installation Introduction

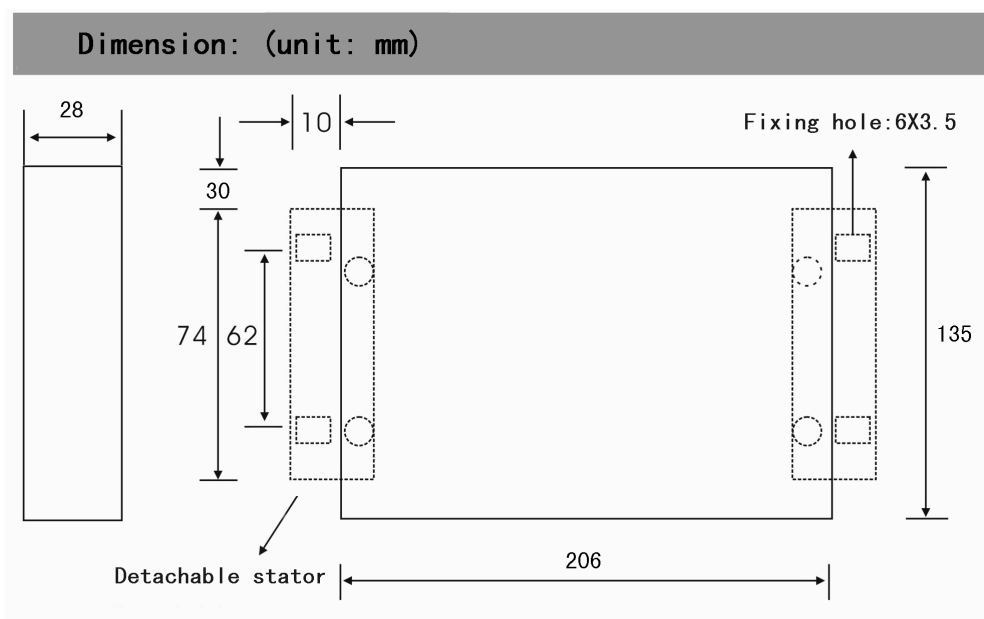
2.1. General

You should review the router configuration immediately after installation to ensure all settings are as desired. Failure to do so may result in unauthorized access to your equipment.

2.2. Package Contents

Name	Quantity	Remark
Router host	1	
Cellular antenna (Male SMA)	1	
WIFI antenna (Female SMA)	1	
GPS antenna (Male SMA)	1	
Network cable	1	
Console cable	1	optional
Power adapter	1	
Manual CD	1	
Certification card	1	
Maintenance card	1	

2.3. Installation and Cable Connection



2.4. Accessories List

Name	Quantity
Router	1
Cellular Antenna	1
GPS Antenna	1
WIFI Antenna	1
Network cable	1
Serial cable	1
Power Lead	1
Stator	2

2.5. SIM card Installation

Power off the router, and press the eject button next to the SIM card tray with a small object such as a ballpoint pen. The SIM card tray will eject from the face of the modem. Place the SIM card into the SIM card tray (Ensure that the side of the SIM card with the metal connection points is facing away from the tray), and then insert the SIM card tray back into the SIM card outlet.

2.6. Antenna Installation

Attach the SMA male connector of the cellular antenna into the female SMA interface on the router labeled "Antenna".

Attach the SMA male connector of the WIFI antenna into the female SMA interface on the router labeled "WIFI".

The router supports an RS232 interface and a 10/100M Ethernet interface. These two interfaces both utilize an RJ45 connector, with the RS232 interface labeled "Console" and the 10/100M Ethernet interface labeled "ETH".

Plug the RJ45 end of the serial cable into the RJ45 outlet of the router labeled "console", and plug the DB9F end of the serial cable into the RS232 serial interface of the user's device.

The pin-out connections of the serial cable are as follows:

RJ45	DB9F
1	8
2	6
3	2
4	1
5	5
6	3
7	4
8	7

The signal definition of the DB9F serial communication interface is as follows:

Pin	RS232 signal	Direction
1	DCD	Output
2	RXD	Output
3	TXD	Input
4	DTR	Input
5	GND	
6	DSR	output
7	RTS	input
8	CTS	output

2.7. Power

The input supply voltage range is 5~35VDC. We recommend using the standard DC 12VDC/1.5A power adaptor available from Maxon.

2.8. Indicator Lights Introduction

The router provides following indicator lights: "Power", "System", "Online", "GPS", "Local Network", "WAN", "WIFI", "Signal Strength".

Indicator Light	State	Introduction
Power	ON	Router is powered on
	OFF	Router is powered off
System	BLINK	Router is up and working
	OFF	Router is not currently working
Online	ON	Router has logged on network
	OFF	Router hasn't logged on network
GPS	ON	WLAN is not active
	OFF	WLAN is active
Local Network	OFF	The corresponding interface of switch is not connected
	ON / BLINK	The corresponding interface of switch is connected /Communicating
WAN	OFF	The WAN interface is unplugged
	ON / BLINK	The WAN interface is plugged in/data is traversing the WAN interface
WIFI	OFF	WIFI is not active
	ON	WIFI is active
Signal Strength	One Light ON	Signal strength is weak
	Two Lights ON	Signal strength is medium
	Three Lights ON	Signal strength is good

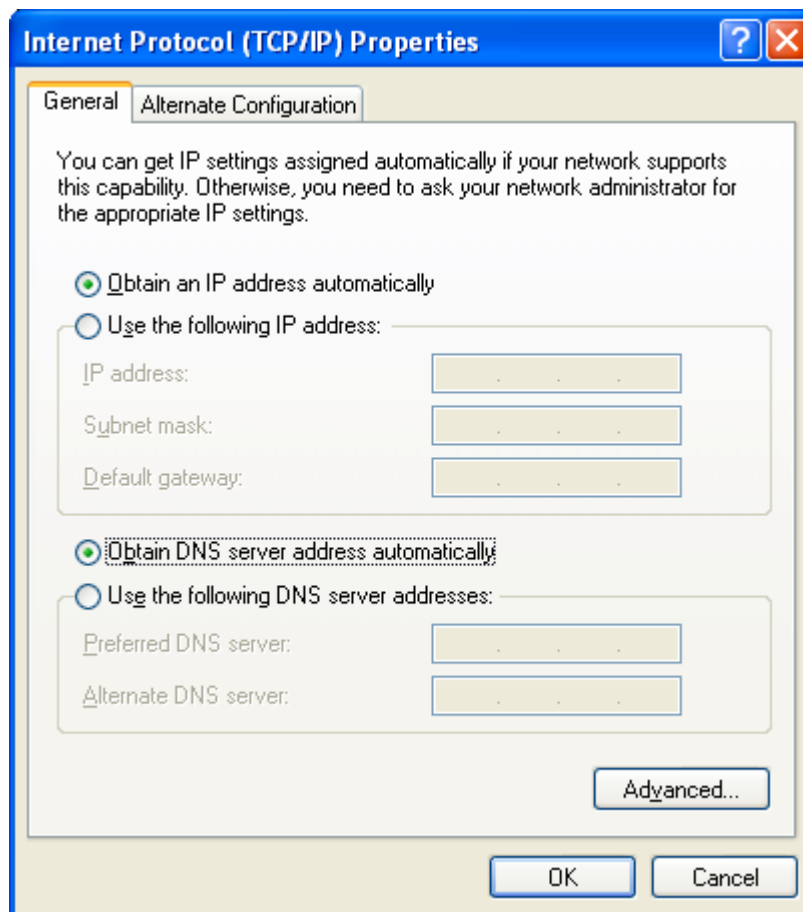
2.9. Reset Button

The modems "Reset" button is used to restore the modem to its original factory default settings. To restore the router to factory default settings, the user needs to press the "Reset" button and hold it in for 15s, the router will then restore its original factory default settings and restart automatically. Note that the reset button is recessed to prevent accidental resets – to press, use a small blunt object such as a ballpoint pen.

3. Configuration and Management

Datamax+ is configured via a web interface. In order to access the Datamax+ web interface you will need a computer with a spare Ethernet LAN port. The LAN card configuration should have the Internet Protocol TCP/IP set to obtain an IP Address automatically and obtain DNS server address automatically.

To check these settings go to your LAN adaptor properties and check your Internet Protocol TCP/IP settings, it should look as follows:



Connection Steps:

1. Connect the Ethernet cable supplied with your router to your computer Ethernet LAN port
2. Your computer will get an IP address from the Datamax+ DHCP range automatically.
3. In your web browser type 192.168.1.1 in the Address (URL) field (The Default IP Address of the Ethernet port is 192.168.1.1). The router will prompt you to change the login credentials, the default username and password are both “admin”.

Router Management

Your Router is currently not protected and uses an unsafe default username and password combination, please change it using the following dialog!

Router Password

Router Username	<input type="text" value="admin"/>
Router Password	<input type="password" value="•••••"/>
Re-enter to confirm	<input type="password" value="•••••"/>

Change Password

After access to the information main page

Menu
Setup
Wireless
Services
VPN
Security
NAT
Access Restrictions
QoS Setting
Applications
Administration
Status

System Information

Router

Router Name	Router
Router Model	Router
LAN MAC	00:0C:43:9C:5A:B9
WAN MAC	00:0C:43:9C:5A:BA
Wireless MAC	00:0C:43:9C:5A:BB
WAN IP	123.209.7.114
LAN IP	192.168.1.1

Services

DHCP Server	Enabled
ff-radauth	Disabled
USB Support	Enabled

Memory

Total Available	59.3 MB / 64.0 MB
Free	34.3 MB / 59.3 MB
Used	25.0 MB / 59.3 MB
Buffers	2.9 MB / 25.0 MB
Cached	9.2 MB / 25.0 MB
Active	1.3 MB / 25.0 MB
Inactive	2.2 MB / 25.0 MB

Wireless

Radio	Radio is On
Mode	AP
Network	Mixed
SSID	ssid
Channel	6 (2437 MHz)
TX Power	71 mW
Rate	72 Mb/s

Wireless Packet Info

Received (RX)	918 OK, no error
Transmitted (TX)	15 OK, no error

Wireless

Clients

MAC Address	Interface	Uptime	TX Rate	RX Rate	Signal	Noise	SNR	Signal Quality
- None -								

DHCP

DHCP Clients

Host Name	IP Address	MAC Address	Client Lease Time
- None -			

3.1. Management and configuration

3.1.1. Setting

The Setup screen is the first screen users will see when accessing the router. Most users will be able to configure the router and get it work properly using only the settings on this screen. Some Internet Service Providers (ISPs) will require users to enter specific information, such as User Name, Password, IP Address, Default Gateway Address, or DNS IP Address. This information can be obtained from your ISP, if required.

3.1.1.1. Basic Setting

WAN Connection Type

There are seven configuration options for the WAN interface:

Disabled; Static IP; Automatic Configuration using one of DHCP, PPPOE, PPTP, L2TP, 3G/UNMTS/4G/LTE

Disabled

Connection Type Disabled

The WAN port is not used

Static IP

Connection Type Static IP

WAN IP Address	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Subnet Mask	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Gateway	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Static DNS 1	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Static DNS 2	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Static DNS 3	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

WAN IP Address: IP address of the WAN interface

Subnet Mask: subnet mask of the WAN interface

Gateway: the default gateway address

Static DNS1/DNS2/DNS3: upstream DNS server IP addresses

Note that for use in your own internal network, your network administrator can supply these details. Where you are using an ISP or other upstream service provider, that supplier can supply you with the required details.

Automatic Configuration-DHCP

Connection Type Automatic Configuration - DHCP

IP address, netmask and default gateway of WAN port are all set automatically via DHCP

PPPOE

Connection Type PPPoE

User Name

Password ☐ Unmask

Service Name

PPP Compression (MPPC) ☐ Enable ☒ Disable

T-Home VDSL VLAN 7/8 Tagging ☐ Enable ☒ Disable

MPPE Encryption

Single Line Multi Link ☐

User Name: Your username (typically supplied by your ISP)

Password: Your password (typically supplied by your ISP)

Service Name: If required by your ISP, otherwise leave blank.

PPP Compression (MPPC): If your ISP supports compression and you wish you use it, it can be enabled here

T-Home VDSL VLAN 7/8 Tagging: If your ISP supports VDSL, you can enable it here.

MPPE Encryption: if your connection requires Microsoft point to point encryption, shared key is entered here.

Single Line Multi Link: enable single line link or disable multi-link

Invalid PPP password characters list:

“(double quotation mark)

’(quotation mark)

?(question mark)

)(bracket)

@(at sign)

;(semi colon)

|(pipe sign)

l(upper case l)

PPTP

The WAN interface creates a PPTP connection to use instead of “raw” access.

Connection Type	<input type="text" value="PPTP"/>
Use DHCP	<input type="radio"/> Yes <input checked="" type="radio"/> No
WAN IP Address	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Subnet Mask	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Gateway	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Gateway (PPTP Server)	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/> <input type="checkbox"/> Unmask
PPTP Encryption	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Disable Packet Reordering	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Additional PPTP Options	<div><div></div></div>

Use DHCP: automatic (“yes”) or manual (“no”) configuration of IP address, subnet mask and default gateway.

Gateway (PPTP Server): The IP address of the PPTP server (your ISP will provide this)

User Name: your username as supplied by your ISP

Password: your password as supplied by your ISP

PPTP Encryption: encrypt (secure) packets over the PPTP link – your ISP will advise if this is required.

Disable Packet Reordering: This option can increase link throughput, however your ISP must support this function.

Additional PPTP Options: any extra options that your ISP requires that are not listed elsewhere can be set here.

L2TP

The WAN link will be a layer 2 tunneling protocol link connected across the WAN interface as defined.

Connection Type	<input type="text" value="L2TP"/>	
User Name	<input type="text"/>	
Password	<input type="text"/>	<input type="checkbox"/> Unmask
Gateway (L2TP Server)	<input type="text"/>	
Require CHAP	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Refuse PAP	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Require Authentication	<input checked="" type="radio"/> Yes <input type="radio"/> No	

User Name: your username as supplied by your ISP or network administrator

Password: your password as supplied by your ISP or network administrator

Gateway (L2TP Server): The IP address of the L2TP server you wish to connect to

Require CHAP: Force CHAP based authentication

Refuse PAP: Prevent PAP based authentication

Require Authentication: L2TP server requires authentication

3G/UMTS/4G/LTE

The WAN connection will be 2G/3G/4G on the Datamax.

Connection Type	<input type="text" value="3G/UMTS/4G/LTE"/>	
User Name	<input type="text"/>	
Password	<input type="text"/>	<input type="checkbox"/> Unmask
Dial String	<input type="text" value="*99***1# (UMTS/3G/3.5G)"/>	
APN	<input type="text"/>	
PIN	<input type="text"/>	<input type="checkbox"/> Unmask

User Name: your username (if any) as supplied by your mobile service provider

Password: your password (if any) as supplied by your mobile service provider

Dial String: the number to dial to get a data connection as supplied by your mobile service provider

APN: access point name as supplied by your mobile service provider

PIN: if your SIM card is PIN protected, you can enter the PIN here

Connection type

Connection type

Connection type: Auto, Force 4G, Force 3G, Force 2G, Prefer 3G, Prefer 2G options. In most cases Auto is preferred, however in some circumstances and locations, you can gain reliability and/or speed advantages by forcing particular connection options.

Keep Online

Keep Online Detection

Detection Interval Sec.

Primary Detection Server IP

Backup Detection Server IP

This function is used to monitor your WAN connectivity so that “broken” connections can be re-established, or alternate connections established.

Detection Method:

None: do not monitor connectivity.

Ping: Send ICMP Echo requests to the primary and backup detection server address

Route: Detect connection with route method, when choose this method, users should also configure "Detection Interval", "Primary Detection Server IP" and "Backup Detection Server IP" items.

PPP: Detect connection with PPP method, when choose this method, users should also configure "Detection Interval" item.

Detection Interval: time (in seconds) to wait between detection attempts.

Primary Detection Server IP: the primary (first) server that should be reachable and respond to the configured detection method

Backup Detection Server IP: the backup (second) server that should be reachable via the WAN interface and respond to the configured detection method

Note: Both the primary and backup detection servers should be stable and reliable – if these servers fail to respond correctly in a timely manner, the modem will attempt to drop and re-establish the connection. During this time, no incoming or outgoing traffic can be send/received.

Connection Strategy

Connection Strategy

☐ Connect on Demand: Max Idle Time Min.
☒ Keep Alive: Redial Period Sec.

Connection Strategy:

'Connect on Demand' only connects to your mobile service provider when there is outgoing data being sent. The connection is dropped when there is no WAN traffic for the 'Max Idle Time' period. While this saves power and possibly reduces mobile service provider charges, your equipment (including the Datamax modem) will not be reachable via the WAN interface when the connection has been dropped.

'Keep Alive' tries to maintain a WAN connection at all times, allowing you to interrogate your equipment at any time, rather than waiting for it to report to you.

Force reconnect

☒ Enable ☐ Disable

Time

Force reconnect: Enabling this option forces the Datamax to drop the WAN connection and then re-establish it at the defined interval.

Time: the time between forced reconnects.

STP

STP

☐ Enable ☒ Disable

STP (Spanning Tree Protocol) allows for multiple redundant links while preventing routing loops – packets do not “ping-pong” from router to router.

Optional Configuration

Router Name	<input type="text" value="Datamax MA100-1010"/>
Host Name	<input type="text"/>
Domain Name	<input type="text"/>
MTU	<div><div>Auto</div><div>1500</div></div>

Router Name: set router name

Host Name: the host name part of the FQDN of the Datamax

Domain Name: the domain part of the FQDN of the Datamax

MTU: Maximum (user) data size in packets sent. Usually “auto”, however depending on your ISP and/or local network settings, you may need to reduce this – please contact your network administrator and/or ISP.

Router Internal Network Settings

Router IP

Local IP Address	<input type="text" value="192"/>	<input type="text" value="168"/>	<input type="text" value="1"/>	<input type="text" value="1"/>
Subnet Mask	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>
Gateway	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Local DNS	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

Local IP Address: IP address of the routers LAN interface

Subnet Mask: the subnet mask of the routers LAN interface

Gateway: the default gateway address [for LAN clients](#)

Local DNS: Normally set to auto to use the nameservers your upstream provider supplies (eg, by DHCP), however you may wish to use your own nameservers to resolve host names on your private network.

Network Address Server Settings (DHCP)

The Datamax can act as a DHCP server for (W)LAN connected devices. It can also act as a DHCP forwarder where you are utilizing a central DHCP server for multiple sites (subnets).

DHCP Type	<div>DHCP Server</div>
DHCP Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Start IP Address	192.168.1. <div>100</div>
Maximum DHCP Users	<div>50</div>
Client Lease Time	<div>1440</div> minutes
Static DNS 1	<div>0</div> . <div>0</div> . <div>0</div> . <div>0</div>
Static DNS 2	<div>0</div> . <div>0</div> . <div>0</div> . <div>0</div>
Static DNS 3	<div>0</div> . <div>0</div> . <div>0</div> . <div>0</div>
WINS	<div>0</div> . <div>0</div> . <div>0</div> . <div>0</div>
Use DNSMasq for DHCP	<input checked="" type="checkbox"/>
Use DNSMasq for DNS	<input checked="" type="checkbox"/>
DHCP-Authoritative	<input checked="" type="checkbox"/>

DHCP Type: select DHCP Server or DHCP Forwarder as appropriate
When you select DHCP Forwarder, you will see input fields for the IP address of the remote DHCP server as below:

DHCP Type	<div>DHCP Forwarder</div>
DHCP Server	<div>0</div> . <div>0</div> . <div>0</div> . <div>0</div>

DHCP Server: enable or disable the DHCP server

Start IP Address: the first (lowest) IP address to issue when a DHCP request comes in – make sure you exclude the Datamax IP address!

Maximum DHCP Users: the maximum number of concurrent DHCP leases allowed

Client Lease Time: the time the IP address is leased for in minutes. After this amount of time, the client will need to acquire a new lease if it wishes to remain connected.

Static DNS (1-3): If you wish to use your own DNS servers, you can enter their IP addresses here. Leave blank to use WAN configured DNS servers.

WINS: if you are using a WINS server for name resolution, you can enter its IP address here.

DNSMasq: users' domain name in the field of local search, increase the expansion of the host option, to adopt DNSMasq can assign IP addresses and DNS for the subnet, if select DNSMasq, dhcpd service is used for the subnet IP address and DNS.

Time Settings

Select time zone of your location. To use local time, leave the checkmark in the box next to Use local time.

NTP Client	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Time Zone	UTC+08:00 ▼
Summer Time (DST)	last Sun Mar - last Sun Oct ▼
Server IP/Name	<input type="text"/>

NTP Client: Get the system time from NTP server

Time Zone: Time zone options

Summer Time (DST): set it depends on users' location

Server IP/Name: IP address of NTP server, up to 32 characters. If blank, the system will find a server by default

Adjust Time

Time	<input type="text" value="2012"/> - <input type="text" value="3"/> - <input type="text" value="15"/>	<input type="text" value="9"/> : <input type="text" value="16"/> : <input type="text" value="20"/>	<input type="button" value="Get"/>	<input type="button" value="Set"/>
------	--	--	------------------------------------	------------------------------------

Where you are not using NTP, or the NTP server is currently unreachable, you can set the routers real-time clock here. Click the “get” button to refresh the browser page with the current router time and “Set” to set the current router time.

3.1.1.2. Dynamic DNS

For users that have a dynamically assigned IP address, a DNS server that supports dynamic DNS updates will allow you to refer to your devices by name and have them continue to connect correctly even when the IP address of the device changes. The Datamax+ router supports dynamic DNS updates, automatically updating the DNS server when the WAN interface IP address assignment changes.

DDNS Service: The Maxon MA100-1010 router currently supports DynDNS, freedns, Zoneedit, NO-IP, 3322, easyDNS, TZO, DynSIP and Custom based on the user.

DDNS Service	<input type="text" value="3322.org"/>	<input type="button" value="v"/>
User Name	<input type="text"/>	
Password	<input type="password"/>	<input type="checkbox"/> Unmask
Host Name	<input type="text"/>	
Type	<input type="text" value="Dynamic"/>	<input type="button" value="v"/>
Wildcard	<input type="checkbox"/>	
Do not use external ip check	<input checked="" type="radio"/> Yes	<input type="radio"/> No

User Name: your DDNS server username

Password: your DDNS server password

Host Name: the FQDN of the DDNS server

Type: select the appropriate value (list varies depending on the setting of "DDNS Service")

Wildcard: support wildcard or not, the default is OFF. ON means

*.host.3322.org is equal to host.3322.org

Do not use external ip check: enable or disable the function of 'do not use external ip check'

Force Update Interval	<input type="text" value="10"/>	(Default: 10 Days, Range: 1 - 60)
-----------------------	---------------------------------	-----------------------------------

Force Update Interval: How often (in days) to force a DDNS update, even if the IP address hasn't changed.

Status

DDNS Status

```
Fri Nov 25 13:58:32 2011: INADYN: Started 'INADYN Advanced version 1.96-ADV' - dynamic DNS updater.  
Fri Nov 25 13:58:32 2011: INADYN: IP read from cache file is '192.168.8.222'. No update required.  
Fri Nov 25 13:58:32 2011: I:INADYN: IP address for alias 'testsixin.3322.org' needs update to '192.168.8.38'  
Fri Nov 25 13:58:33 2011: I:INADYN: Alias 'testsixin.3322.org' to IP '192.168.8.38' updated successfully.
```

DDNS Status shows DDNS specific log information

3.1.1.3. Clone MAC Address

Some ISPs lock service provision to a MAC address. By cloning the MAC address, you can insert the Datamax into the network path without needing to update your MAC address with your ISP.

☒ Enable ☐ Disable

Clone LAN MAC

00 : AA : BB : CC : DD : 43

Clone WAN MAC

00 : AA : BB : CC : DD : 44

[Get Current PC MAC Address](#)

Clone Wireless MAC

00 : AA : BB : CC : DD : 45

Clone MAC address can clone three parts: Clone LAN MAC, Clone WAN MAC, Clone Wireless MAC.

Note: MAC addresses are 48 characters, they cannot be set to a multicast address, and the first byte must be even. The MAC address value of network bridge br0 is determined by the lower order bits of wireless MAC address and LAN port MAC address.

3.1.1.4. Advanced Router

Operating Mode: Gateway and Router

Operating Mode

Operating Mode

Gateway ▼

If the Datamax is acting as your primary gateway to the internet, select “gateway”, otherwise select “router”.

Dynamic Routing

Dynamic Routing

Interface	Disable
-----------	---------

If you want the router to participate in dynamic routing protocols such as RIP etc running on your network(s), you should enable this option. To enable the Dynamic Routing feature for the WAN side, select WAN. To enable this feature for the LAN and wireless side, select LAN&WLAN. To enable the feature for both the WAN and LAN, select Both. To disable the Dynamic Routing feature for all network interfaces, keep the default setting, Disable.

Note : Dynamic Routing is not available in Gateway mode

Static Routing

Static Routing

Select set number

1 ()

Delete

Route Name

Metric

0

Destination LAN NET

0

.

0

.

0

.

0

Subnet Mask

0

.

0

.

0

.

0

Gateway

0

.

0

.

0

.

0

Interface

LAN & WLAN

Show Routing Table

Select set number: the routing table entry number

Route Name: naming rules makes your life easier!

Metric: the “cost” of this route – lower numbers are preferred routes.

Destination LAN NET: the new route destination address

Subnet Mask: the subnet mask for the new route

Gateway: IP address of the gateway device that forwards packets to the destination host or network.

Interface: The interface that has the gateway attached (LAN/WLAN, WAN, or loopback)

Show Routing Table

Routing Table Entry List			
Destination LAN NET	Subnet Mask	Gateway	Interface
192.168.1.1	255.255.255.255	0.0.0.0	WAN
192.168.1.0	255.255.255.0	0.0.0.0	LAN & WLAN
192.168.1.0	255.255.255.0	0.0.0.0	WAN
169.254.0.0	255.255.0.0	0.0.0.0	WAN
0.0.0.0	0.0.0.0	192.168.1.1	LAN & WLAN

Refresh

Close

3.1.1.5. VLANs

VLAN

VLAN	Port					Assigned To Bridge
	W	1	2	3	4	
0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LAN <input type="button" value="v"/>
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>

VLAN's allow you to specify which ports are “bridged” – that is, where broadcast traffic will be shared for example – rather than routed. This allows you to create separate subnets on each LAN port (or group of LAN ports). Note that although there are 15 VLAN's available, there are only 5 ports (4 x LAN, 1 x WAN). Note also that the WAN port should be on a separate VLAN or routing to the WAN may not work.

3.1.1.6. Networking

Bridging

Create Bridge

Bridge 0
 STP Prio MTU

Assign to Bridge

Current Bridging Table

Bridge Name	STP enabled	Interfaces
br0	no	vlan0 ra0

Auto Refresh is On

Bridging-Create Bridge: creates a new empty network bridge for later use. STP means Spanning Tree Protocol and with PRIO users are able to set the bridge priority order. The lowest number has the highest priority.

Bridging - Assign to Bridge: allows users to assign any valid interface to a network bridge. Consider setting the Wireless Interface options to Bridged if they want to assign any Wireless Interface here. Any system specific bridge setting can be overridden here in this field.

Current Bridging Table: shows current bridging table

Create steps as below:

Click 'Add' to create a new bridge, configuration is as below:

Create Bridge

Bridge 0
 STP Prio MTU
Bridge 1
 STP Prio MTU

Create bridge option: the first br0 means bridge name. STP means to on/off spanning tree protocol. Prio means priority level of STP, the smaller the number, the higher the level. MTU means maximum transfer unit, default is 1500, delete if it is not need. And then click 'Save' or 'Add'. Bridge properties are as below:

Create Bridge

Bridge 0	br0	STP Off	Prio 32768	MTU 1500	Delete
Bridge 1	br1	STP On	Prio 32768	MTU 1500	Delete
IP Address	0.0.0.0				
Subnet Mask	0.0.0.0				
Add					

Enter relevant bridge IP address and subnet mask, click 'Add' to create a bridge.

Note: Only create a bridge can apply it.

Assign to Bridge

Assignment 0	none	Interface ra0	Prio 63	Delete
Add				

Assign to Bridge option: to assign different ports to created bridge. For example: assign port (wireless port) is ra0 in br1 bridge as below:

Prio means priority level: work if multiple ports are within the same bridge. The smaller the number, the higher the level. Click 'Add' to take it effect.

Note: corresponding interface of WAN ports interface should not be binding, this bridge function is basically used for LAN port, and should not be binding with WAN port

If bind success, bridge binding list in the list of current bridging table is as below:

Current Bridging Table

Bridge Name	STP enabled	Interfaces
br0	no	vlan0
br1	yes	ra0

Auto-Refresh is On

To make br1 bridge has the same function with DHCP assigned address, users need to set multiple DHCP function, see the introduction of multi-channel DHCPD:

Port Setup

Network Configuration eth2	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration vlan0	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration ra0	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration apcli0	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration wds0	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration wds1	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration wds2	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration wds3	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration br0	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default

Port Setup: Set the port property, the default is not set

Network Configuration ra0	<input checked="" type="radio"/> Unbridged	<input type="radio"/> Default
MTU	<input type="text" value="1500"/>	
Multicast forwarding	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Masquerade / NAT	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
IP Address	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>	
Subnet Mask	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>	

Choose not bridge to set the port's own properties, detailed properties are as below:

MTU: maximum transfer unit

Multicast forwarding: enable or disable multicast forwarding

Masquerade/NAT: enable or disable Masquerade/NAT

IP Address: set ra0's IP address, and do not conflict with other ports or bridge

Subnet Mask: set the port's subnet mask

Multiple DHCP Server

DHCP 0	<input type="text" value="ra0"/>	<input type="text" value="On"/>	Start	<input type="text" value="100"/>	Max	<input type="text" value="50"/>	Leasetime	<input type="text" value="3600"/>
<input type="button" value="Delete"/>								
<input type="button" value="Add"/>								

Multiple DHCPD: using multiple DHCP service. Click 'Add' in multiple DHCP server to appear relevant configuration. The first means the

name of port or bridge (do not be configured as eth0), the second means whether to on DHCP. Start means start address, Max means maximum assigned DHCP clients, Leasetime means the client lease time, the unit is second, click 'Save' or 'Apply' to put it into effect after setting.

Note: You can only create one DHCP instance at a time – please press “Save” or “Apply” after each instance creation to be able to specify the next instance.

3.1.2. Wireless

3.1.2.1. Basic Settings

Wireless Physical Interface wl0 [2.4 GHz]

Wireless Network

☒ Enable ☐ Disable

Physical Interface ra0 - SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]

Wireless Mode

AP

Wireless Network Mode

N-Only

802.11n Transmission Mode

Mixed

Wireless Network Name (SSID)

dd-junjinlee

Wireless Channel

11 - 2.462 GHz

Channel Width

40 MHz

Extension Channel

upper

Wireless SSID Broadcast

☒ Enable ☐ Disable

Network Configuration

☐ Unbridged ☒ Bridged

Virtual Interfaces

Add

Save

Apply Settings

Cancel Changes

Wireless Network : “Enable” or “Disable” the WiFi of the router.

Wireless Mode : AP, Client, Adhoc, Repeater, Repeater Bridge.

Wireless Network Mode :

Mixed : Support 802.11b, 802.11g, 802.11n wireless devices.

BG-Mixed : Support 802.11b, 802.11g wireless devices.

B-only : Only supports the 802.11b standard wireless devices.

G-only : Only supports the 802.11g standard wireless devices.

NG-Mixed : Support 802.11g, 802.11n wireless devices.

N-only : Only supports the 802.11g standard wireless devices.

802.11n Transmission Mode : In the wireless network mode "N-only", you can select:

Greenfield: If no other WiFi coverage is in the area, this mode will increase throughput. However, when this mode is used where other WiFi is present, throughput will decrease.

Mixed : When other WiFi coverage is in the area, this mode reduces errors. However, when used where no other WiFi is available, this decreases throughput.

Wireless Network Name(SSID): The SSID is the network name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all devices in your wireless network.

Wireless Channel : A total of 1-13 channels to choose more than one wireless device environment, please try to avoid using the same channel with other devices.

Channel Width : 20MHZ and 40MHZ.

Extension Channel : Channel for 40MHZ, you can choose upper or lower.

Wireless SSID Broadcast :

Enable : SSID is announced and advertised by the router

Disable : SSID is not advertised – you cannot “browse” this network to connect, you must know it exists.

Network Configuration :

Bridged : Bridge to the router, under normal circumstances, please select the bridge.

Unbridged : There is no bridge to the router, IP addresses need to manually configure.

Network Configuration	<input checked="" type="radio"/> Unbridged <input type="radio"/> Bridged
Multicast forwarding	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Masquerade / NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IP Address	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="1"/> <input type="text" value="1"/>
Subnet Mask	<input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="0"/> <input type="text" value="0"/>

Virtual Interfaces : Click Add to add a virtual interface. Add successfully, click on the remove, you can remove the virtual interface.

Virtual Interfaces

Virtual Interfaces ra1 SSID [dd-wrt_vap] HWAddr [00:AA:BB:CC:DD:16]

Wireless Network Name (SSID)	<input type="text" value="dd-wrt_vap"/>
Wireless SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Network Configuration	<input type="radio"/> Unbridged <input checked="" type="radio"/> Bridged

Add Remove

AP Isolation : This setting isolates wireless clients so access to and from other wireless clients are stopped.

Note : Save your changes, after changing the "Wireless Mode", "Wireless Network Mode", "wireless width", "broadband" option, please click on this button, and then configure the other options.

3.1.2.2. Wireless Security

Wireless security options used to configure the security of your wireless network. This route is a total of seven kinds of wireless security mode. Disabled by default, not safe mode is enabled. Such as changes in Safe Mode, click Apply to take effect immediately.

Wireless Security wl0

Physical Interface ra0 SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]

Security Mode	<input type="text" value="Disabled"/>
---------------	---------------------------------------

Save Apply Settings

Wireless Security wlo

Physical Interface ra0 SSID [four-faith] HWAddr [00:0C:43:30:52:79]

Security Mode	<input type="text" value="WEP"/>
Authentication Type	<input checked="" type="radio"/> Open <input type="radio"/> Shared Key
Default Transmit Key	<input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4
Encryption	<input type="text" value="64 bits 10 hex digits/5 ASCII"/>
ASCII/HEX	<input type="radio"/> ASCII <input checked="" type="radio"/> HEX
Passphrase	<input type="text" value="1111111111111111"/> <input type="button" value="Generate"/>
Key 1	<input type="text" value="2627F68597"/>
Key 2	<input type="text" value="15AD1DD294"/>
Key 3	<input type="text" value="DDC4761939"/>
Key 4	<input type="text" value="31F1ADB558"/>

WEP : Is a basic encryption algorithm is less secure than WPA. Use of WEP is discouraged due to security weaknesses, and one of the WPA modes should be used whenever possible. Only use WEP if you have clients that can only support WEP (usually older, 802.11b-only clients).

Authentication Type : Open or shared key.

Default Transmit Key : Select the key form Key 1 - Key 4 key.

Encryption : There are two levels of WEP encryption, 64-bit (40-bit) and 128-bit. To utilize WEP, select the desired encryption bit, and enter a passphrase or up to four WEP key in hexadecimal format. If you are using 64-bit (40-bit), then each key must consist of exactly 10 hexadecimal characters or 5 ASCII characters. For 128-bit, each key must consist of exactly 26 hexadecimal characters. Valid hexadecimal characters are "0"-"9" and "A"-"F".

ASCII/HEX: ASCII, the keys is 5 bit ASCII characters/13bit ASCII characters.
HEX, the keys is 10bit/26 bit hex digits.

Passphrase : The letters and numbers used to generate a key.

Key1-Key4 : Manually fill out or generated according to input the pass phrase.

Wireless Security wlo

Physical Interface ra0 SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]

Security Mode WPA Personal ▼

WPA Algorithms AES ▼

WPA Shared Key

☐ Unmask

Key Renewal Interval (in seconds)

(Default: 3600, Range: 1 - 99999)

Save
Apply Settings

WPA Personal/WPA2 Personal/WPA2 Person

Mixed:, TKIP/AES/TKIP+AES, dynamic encryption keys. TKIP + AES, self-applicable TKIP or AES. WPA Person Mixed, allows WPA Personal and WPA2 Personal client mix.

WPA Shared Key : Between 8 and 63 ASCII character or hexadecimal digits.。

Key Renewal Interval (in seconds) : 1-99999.。

Wireless Security wlo

Physical Interface ra0 SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]

Security Mode WPA Enterprise ▼

WPA Algorithms AES ▼

Radius Auth Server Address
.
.
.

Radius Auth Server Port

(Default: 1812)

Radius Auth Shared Secret

☐ Unmask

Key Renewal Interval (in seconds)

WPA Enterprise/WPA2 Enterprise/WPA2 Enterprise Mixed: WPA Enterprise uses an external RADIUS server to perform user authentication.

WPA Algorithms: AES/TKIP/TPIP+AES.

Radius Auth Sever Address : The IP address of the RADIUS server.

Radius Auth Server Port : The RADIUS Port (default is 1812)。

Radius Auth Shared Secret : The shared secret from the RADIUS server.。

Key Renewal Interval(in seconds): 1-99999.。

Wireless Security wl0

Physical Interface ra0 SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]

Security Mode	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">802.1x</div>
XSupplicant Type	<input type="radio"/> Peap <input checked="" type="radio"/> TTLS
User	<div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div>
Anonymous Identity	<div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div>
Password	<div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div>
Phase2	<div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div>
Public Server Certificate	<div style="border: 1px solid #ccc; height: 50px; width: 100%;"></div> <div style="text-align: right; padding-right: 5px;"> <div style="border: 1px solid #ccc; width: 15px; height: 15px; margin-bottom: 2px;"></div> <div style="border: 1px solid #ccc; width: 15px; height: 15px;"></div> </div>
Additional Network Options	<div style="border: 1px solid #ccc; height: 30px; width: 100%;"></div> <div style="text-align: right; padding-right: 5px;"> <div style="border: 1px solid #ccc; width: 15px; height: 15px; margin-bottom: 2px;"></div> <div style="border: 1px solid #ccc; width: 15px; height: 15px;"></div> </div>

802.1x: 802.1x for user to connect to a wireless access point and cable converter to provide the certification. It will limit without obtaining the user credentials to connect to the Internet, credentials - for example, a separate server authentication user name and password.

Peap: PEAP (Protected Extensible Authentication Protocol) is a version of EAP, the authentication protocol used in wireless networks and Point-to-Point connections. PEAP is designed to provide more secure authentication for 802.11 WLANs (wireless local area networks) that support 802.1X port access control. Here is PEAP-EAP-MS-CHAPv2.

1. Enter the User.
2. Enter the Password.

TTLS: TTLS uses the TLS channel to exchange "attribute-value pairs" (AVPs), much like RADIUS. (In fact, the AVP encoding format is very similar to RADIUS.) The general encoding of information allows a TTLS server to validate AVPs against any type of authentication mechanism. TTLS implementations today support all methods defined by EAP, as well as several older methods (CHAP, PAP, MS-CHAP and MS-CHAPv2). TTLS can easily be extended to work with new protocols by defining new attributes to support new protocols.

1. Enter the User.
2. Enter the Password.

3. Enter the Public Server Certificate.

3.1.2.3. Wireless MAC Filter

The Wireless MAC Filter allows you to control which wireless-equipped PCs may or may not communicate with the router depending on their MAC addresses. For information how to get MAC addresses from Windows-PCs, see MAC Address Cloning for detailed instructions.

Wireless MAC Filter

ra0 - MAC Filter

Use Filter ☒ Enable ☐ Disable

Filter Mode ☒ Prevent clients listed from accessing the wireless network
☐ Permit only clients listed to access the wireless network

[Edit MAC Filter List](#)

[Save](#) [Apply Settings](#) [Cancel Changes](#)

Use Filter : Disabled by default. Select Enable to open the Wireless MAC Filter.

Filter Mode :

Prevent client listed from accessing the wireless

network : "blacklist" mode – listed devices are prevented from accessing via WiFi, all other devices are allowed access.

Permit only client listed to accessing the wireless network : "whitelist" mode – only listed devices can access the WiFi, all other devices are denied access.

You can edit (add, remove etc) device MAC addresses by clicking the "Edit MAC Filter List" button.

3.1.2.4. Advanced Settings

The Wireless Advanced Settings screen allows you to customize data transmission settings. In most cases, these setting can be left at the defaults.

Advanced Wireless Settings

Advanced Settings

Basic Rate	<input type="button" value="Default"/>	(Default: Default)
MIMO - Transmission Fixed Rate	<input type="button" value="Auto"/>	(Default: Auto)
Transmission Fixed Rate	<input type="button" value="Auto"/>	(Default: Auto)
CTS Protection Mode	<input checked="" type="radio"/> Auto <input type="radio"/> Disable	(Default: Auto)
Frame Burst	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Beacon Interval	<input type="text" value="100"/>	(Default: 100ms, Range: 10 - 65535)
DTIM Interval	<input type="text" value="1"/>	(Default: 1, Range: 1 - 255)
Fragmentation Threshold	<input type="text" value="2346"/>	(Default: 2346, Range: 256 - 2346)
RTS Threshold	<input type="text" value="2347"/>	(Default: 2347, Range: 0 - 2347)
Max Associated Clients	<input type="text" value="128"/>	(Default: 128, Range: 1 - 256)
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	(Default: Disable)
TX Antenna	<input type="button" value="Auto"/>	(Default: Auto)
RX Antenna	<input type="button" value="Auto"/>	(Default: Auto)
Preamble	<input type="button" value="Long"/>	(Default: Long)
Shortslot Override	<input type="button" value="Auto"/>	(Default: Auto)
TX Power	<input type="text" value="71"/>	(Default: 71, Range: 1 - 251mW)
Wireless GUI Access	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	(Default: Enable)

Basic Rate : The default value is set to Default. Depending on the wireless mode you have selected, a default set of supported data rates will be selected. The default setting will ensure maximum compatibility with all devices. You may also choose to enable all data rates by selecting ALL. For compatibility with older Wireless-B devices, select 1-2Mbps.

MIMO-Transmission Fixed Rate : The default setting is Auto. The range is from 13.5 to 270Mbps. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or keep the default setting, Auto, to have the router automatically use the fastest possible data rate and enable

the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the router and a wireless client.

Transmission Fixed Rate : The default setting is Auto. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or keep the default setting, Auto, to have the router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the router and a wireless client.

CTS Protection Mode : The default value is disabled. When set to Auto, a protection mechanism will ensure that your Wireless-B devices will connect to the Wireless-G router when many Wireless-G devices are present. However, performance of your Wireless-G devices may be decreased.

Frame Burst : The default value is disabled. Frame burst allows packet bursting which will increase overall network speed though this is only recommended for approx 1-3 wireless clients, Any more clients and there can be a negative result and throughput will be affected.

Beacon Interval : The default value is 100. Enter a value between 1 and 65,535 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the router to synchronize the wireless network. 50 is recommended in poor reception.

DTIM Interval : The default value is 1. This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.

Fragmentation Threshold : This value should remain at its default setting of 2346. The range is 256-2346 bytes. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended.

RTS Threshold : This value should remain at its default setting of 2347. The range is 0-2347 bytes. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.

Max Associated Clients : 1-128.

AP Isolation : The default value is Off. This setting isolates wireless clients so access to and from other wireless clients are stopped.

TX Antenna/ RX Antenna : Values are Auto, Left, Right, default value is Auto. This is used in conjunction with external antennas to give them optimum performance. On some router models left and right antennas may be reversed depending on your point of view.

Preamble : Values are Long and Short, default value is Long. If your wireless device supports the short preamble and you are having trouble getting it to communicate with other 802.11b devices, make sure that it is set to use the long preamble.

Wireless GUI Access: The default value is Enabled. The setting allows access to the routers setup (GUI) from wireless clients. Disable this if you wish to block all wireless clients from accessing the setup pages.

Radio Time Restrictions

Radio Scheduling ☒ Enable ☐ Disable (Default: Disable)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green

Radio Time Restrictions: The *Radio Times Restriction* facility constitutes a time switch for the radio. By default, the time switch is not active and the WLAN is permanently on. Enable the time switch, if you want to turn off the WLAN during some hours of the day. Hours during which the WLAN is on are marked in green, while red indicates that the radio is off. Clicking on the respective hour toggles between on and off.

Wireless Multimedia Support Settings

WMM Support ☒ Enable ☐ Disable (Default: Enable)

No-Acknowledgement ☐ Enable ☒ Disable (Default: Disable)

EDCA AP Parameters (AP to Client)						
	CWmin	CWmax	AIFSN	TXOP(b)	TXOP(a/g)	Admin Forced
Background	15	1023	7	0	0	<input type="checkbox"/>
Best Effort	15	63	3	0	0	<input type="checkbox"/>
Video	7	15	1	6016	3008	<input type="checkbox"/>
Voice	3	7	1	3264	1504	<input type="checkbox"/>

EDCA STA Parameters (Client to AP)						
	CWmin	CWmax	AIFSN	TXOP(b)	TXOP(a/g)	Admin Forced
Background	15	1023	7	0	0	<input type="checkbox"/>
Best Effort	15	1023	3	0	0	<input type="checkbox"/>
Video	7	15	2	6016	3008	<input type="checkbox"/>
Voice	3	7	2	3264	1504	<input type="checkbox"/>

WMM Tx retry limits, fallback limits and max rate parameters.					
	S. Retry	S. Fallbk	L. Retry	L. Fallbk	Max Rate
Background	7	3	4	2	0
Best Effort	7	3	4	2	0
Video	7	3	4	2	0
Voice	7	3	4	2	0

Wireless Multimedia Support Settings: Enable support of Wi-Fi Multimedia feature. Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data

No-Acknowledgement: This refers to the acknowledge policy used at the MAC level. Enabling no-acknowledgement can result in more efficient throughput but higher error rates in a noisy Radio Frequency (RF) environment

EDCA AP Parameters (AP to Client): This affects traffic flowing from the access point to the client station.

EDCA STA Parameters (Client to AP): This affects traffic flowing from the client station to the access point.

Background: Priority is low.

High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).

Best Effort: Priority is Medium.

Medium throughput and delay. Most traditional IP data is sent to this queue.


Video : Priority is High.

Minimum delay. Time-sensitive video data is automatically sent to this queue.

Voice : Priority is High.

Time-sensitive data like VoIP and streaming media are automatically sent to this queue.

CWmin: Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.

 The first random number generated will be a number between 0 and the number specified here. If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window. Valid values for the "cwmin" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmin" must be lower than the value for "CWmax".

Cmax : Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "CWmin".

AIFSN : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames.

TXOP(b)/ TXOP(a/g) : Transmission Opportunity for "a" "b" and "g" modes is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.

3.1.2.5. WDS

WDS (Wireless Distribution System) is a Wireless Access Point mode that enables wireless bridging in which WDS APs communicate only with each other only (without allowing for wireless clients or stations to access them), and/or wireless repeating in which APs communicate both with each other and with wireless stations (at the expense of half the throughput). This firmware currently supports one types of WDS, LAN.

Wireless Distribution System

WDS Settings

Wireless MAC00:AA:BB:CC:DD:15

LAN	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	

Extra Options

Lazy WDS

☐ Enable

☒ Disable

(Default: Disable)

Save

Apply Settings

Cancel Changes

LAN-type WDS

This is the easiest, and currently most common, type of WDS used for linking LANs. It is very simple to setup and requires no extra routing protocols or knowledge of

networking. Simply put, it is pure bridging. A simple example would be extending the range of an existing AP by setting up a 2nd AP and connecting it to the first using LAN-type WDS.

1. Make sure you are using the same Wireless Settings on both routers and not any type of Wireless Security.
2. Find a drop-down selection that has Disabled displayed. Click this and select LAN, do the same on the other router.
3. On the first router, take the numbers next to Wireless MAC and enter them in to the second router on the same line that you set to "LAN".
4. Take the Wireless MAC from the second router and enter them on the first router.
5. Check for any typing errors and then click Save Settings.
6. Go to the Wireless Status page. You should see WDS Link and the Wireless MAC of the other router listed, with a signal reading. If the signal is "0dBm" then there may be something wrong. Check your antenna connections and configuration settings, and try again.
7. Once you have a good signal (-70dBm to -30dBm, -70dBm being lowest), you can change the Internet Connection Type on the Basic Setup page of the second router to Disabled and set the *Gateway* to the LAN IP Address of the first router. You can now run normal tests to check if you are connected (like ping).

Lzay WDS: Default is disabled.

Note : WDS is only available in AP mode. Also Wireless encryption WPA2 and Wireless network mode B-Only are not supported under WDS.

3.1.3. Services

3.1.3.1. Services

DHCP Client

DHCP Client	
Set Vendorclass	<input type="text"/>
Request IP	<input type="text"/>

Set Vendorclass: the DHCP server can automatically identify the specific identifier of the computer running certain operating systems to send, such as the DHCP server can identify the DHCP client running the operating system is Windows 2000 or Windows

98. Identification identifier DHCP option can be assigned to DHCP clients based on specific operating system.

Request IP: IP address of the request

DHCP Server

DHCPd assigns IP addresses to users local devices. While the main configuration is on the setup page users can program some nifty special functions here.

DHCP Server

Use JFFS2 for client lease DB

(Not mounted)

Use NVRAM for client lease DB

☐

Used Domain

WAN

LAN Domain

Additional DHCPd Options

Static Leases

MAC Address	Host Name	IP Address	Client Lease Time
			minutes

Add

Remove

Use NVRAM for client lease DB: The DHCP server will attempt to assign the same IP address to every client it talks to (based on MAC address). Setting this option saves MAC/IP assignments between reboots of the router.

Used domain: users can select here which domain the DHCP clients should get as their local domain. This can be the WAN domain set on the Setup screen or the LAN domain which can be set here.

LAN Domain: users can define here their local LAN domain which is used as local domain for DNSmasq and DHCP service if chose above.

Static Leases: if users want to assign certain hosts a specific address then they can define them here. This is also the way to add hosts with a fixed address to the router's local DNS service (DNSmasq).

Additional DHCPd Options: some extra options users can set by entering them

DNSMasq

DNSmasq is a local DNS server. It will resolve all host names known to the router from dhcp (dynamic and static) as well as forwarding and caching DNS entries from remote DNS servers. *Local DNS* enables DHCP clients on the LAN to resolve static and dynamic DHCP hostnames.

DNSMasq

DNSMasq	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Local DNS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
No DNS Rebind	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Additional DNSMasq Options	<div></div>

Local DNS: enables DHCP clients on the LAN to resolve static and dynamic DHCP hostnames

No DNS Rebind: when enabled, it can prevent an external attacker to access the router's internal Web interface. It is a security measure

Additional DNSMasq Options: some extra options users can set by entering them in Additional DNS Options.

For example:

static allocation: dhcp-

host=AB:CD:EF:11:22:33,192.168.0.10,myhost,myhost.domain,12h

max lease number: dhcp-lease-max=2

DHCP server IP range: dhcp-range=192.168.0.110,192.168.0.111,12h

SNMP

SNMP

SNMP	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable
Location	<input type="text" value="Unknown"/>
Contact	<input type="text" value="root"/>
Name	<input type="text" value="four-faith"/>
RO Community	<input type="text" value="public"/>
RW Community	<input type="text" value="private"/>

Location: equipment location

Contact: contact this equipment management

Name: device name

RO Community: SNMP RO community name, the default is public, Only to read.

RW Community: SNMP RW community name, the default is private, Read-write permissions

SSHD

Enabling SSHd allows users to access the Linux OS of their router with an SSH client

Secure Shell

SSHd	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SSH TCP Forwarding	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Password Login	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Port	<input type="text" value="22"/> (Default: 22)
Authorized Keys	<input type="text"/>

SSH TCP Forwarding: enable or disable to support the TCP forwarding

Password Login: allows login with the router password (username is admin)

Port: port number for SSHd (default is 22)

Authorized Keys: here users paste their public keys to enable key-based login (more secure than a simple password)

System log

Enable Syslogd to capture system messages. By default they will be collected in the local file /var/log/messages. To send them to another system, enter the IP address of a remote syslog server.

System Log

Syslogd	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Syslog Out Mode	<input checked="" type="radio"/> Net <input type="radio"/> Console
Remote Server	<input type="text"/>

Syslog Out Mode: two log mode

Net: the log information output to a syslog server

Console: the log information output to console port

Remote Server: if choose net mode, users should input a syslog server's IP Address and run a syslog server program on it.

Telnet

Telnet

Telnet ☒ Enable ☐ Disable

Telnet: enable a telnet server to connect to the router with telnet. The username is admin and the password is the router's password.

Note: If users use the router in an untrusted environment (for example as a public hotspot), it is strongly recommended to use SSHd and deactivate telnet.

WAN Traffic Counter

WAN Traffic Counter

tttraff Daemon ☒ Enable ☐ Disable

Tttraff Daemon: enable or disable wan traffic counter function

3.1.3.2. PPPoE Server

PPPoE Server

PPPoE Server

RP-PPPoE Server Daemon ☐ Enable ☒ Disable

RP-PPPoEServer Daemon: enable or disable PPPoE server

RP-PPPoEServer Options

RP-PPPoE Server Options

RP-PPPoE Server Interface	LAN	
Client IP(s)	192.168.1.10-100	
Deflate Compression	<input type="checkbox"/>	
BSD Compression	<input type="checkbox"/>	
LZS Stac Compression	<input type="checkbox"/>	
MPPC Compression	<input type="checkbox"/>	
MPPE PPPoE Encryption	<input type="checkbox"/>	
Session Limit per MAC	10	(Default: 10)
LCP Echo Interval	5	(Default: 5)
LCP Echo Failure	12	(Default: 12)
Idle Time	0	(Default: 0 = Deaktivite)
Authentication	<input type="radio"/> Radius <input checked="" type="radio"/> Local User Management (CHAP Secrets)	

PPPOE Server Interface: PPPoE server interface to the outside, only to support the LAN port

Client IP(s): IP range assigns to the PPPoE client in the format: xxx.xxx.xxx.xxx-xxx

Deflate Compression: enable or disable Deflate Compression

BSD Compression: enable or disable BSD Compression

LZS Stac Compression: enable or disable LZS Stac Compression

MPPC Compression: enable or disable MPPC Compression

MPPE PPPoE Encryption: enable or disable MPPE PPPoE Encryption

Session Limit per MAC: default is 10

LCP Echo Interval: time interval to set the the LCP calibration phase response

LCP Echo Failure: release PPPoE over failure times, the PPPoE client will need to reconnect

Idle Time: set idle time, idle time at the appropriate time to release the PPPoE

Authentication: including local and Radius (Remote Authentication Dial In User)

Local User Management (CHAP Secrets)

Local User Management (CHAP Secrets)

User	Password	IP Address	Enable
		0.0.0.0	<input type="checkbox"/>

Add Remove

User: set PPPOE client's user name

Password: set PPPOE client's user password

IP Address: set PPPOE client's user IP address

Enable: enable or disable this setting

Radius

Radius Authentication

Radius Server IP	<input type="text" value="192.168.1.1"/>	
Radius Authentication Port	<input type="text" value="1812"/>	(Default: 1812)
Radius Accounting Port	<input type="text" value="1813"/>	(Default: 1813)
Radius Shared Key	<input type="password" value="••••••••••"/>	

Radius Server IP: set the Remote Authentication Dial In User-Server IP

Radius Authentication Port: set the Remote Authentication Dial in User-Authentication Port

Radius Accounting Port: set the Remote Authentication Dial in User-Accounting Port

Radius Shared Key: transactions between the client and RADIUS accounting server are authenticated through the use of a shared secret, which is never sent over the network.

3.1.4.VPN

3.1.4.1. PPTP

PPTP Server

PPTP Server

PPTP Server ☒ Enable ☐ Disable

Broadcast support ☐ Enable ☒ Disable

Force MPPE Encryption ☒ Enable ☐ Disable

DNS1

DNS2

WINS1

WINS2

Server IP

Client IP(s)

CHAP-Secrets

Broadcast support: enable or disable broadcast support of PPTP server

Force MPPE Encryption: enable or disable force MPPE encryption of PPTP data

DNS1/DNS2/WINS1/WINS2: set DNS1/DNS2/WINS1/WINS2

Server IP: input IP address of the router as PPTP server, differ from LAN address

Client IP(s): IP address assigns to the client, the format is xxx.xxx.xxx.xxx-xxx

CHAP Secrets: user name and password of the client using PPTP service

Note: client IP must be different with IP assigned by router DHCP.

The format of CHAP Secrets is user * password *.

PPTP Client

PPTP Client

PPTP Client Options ☒ Enable ☐ Disable

Server IP or DNS Name

Remote Subnet . . .

Remote Subnet Mask . . .

MPPE Encryption

MTU (Default: 1450)

MRU (Default: 1450)

NAT ☒ Enable ☐ Disable

User Name

Password ☐ Unmask

Server IP or DNS Name: PPTP server's IP Address or DNS Name

Remote Subnet: the network of the remote PPTP server

Remote Subnet Mask: subnet mask of remote PPTP server

MPPE Encryption: enable or disable Microsoft Point-to-Point Encryption。

MTU: maximum Transmission Unit

MRU: maximum Receive Unit

NAT: network Address Translation

User Name: user name to login PPTP Server.

Password: password to log into PPTP Server.

3.1.4.2. L2TP

L2TP Server

L2TP Server

L2TP Server Options ☒ Enable ☐ Disable

Force MPPE Encryption ☒ Enable ☐ Disable

Server IP

Client IP(s)

CHAP-Secrets

Force MPPE Encryption: enable or disable force MPPE encryption of L2TP data

Server IP: input IP address of the router as PPTP server, differ from LAN address

Client IP(s): IP address assigns to the client, the format is xxx.xxx.xxx.xxx-
xxx.xxx.xxx.xxx

CHAP Secrets: user name and password of the client using L2TP service

Note: client IP must be different with IP assigned by router DHCP.

The format of CHAP Secrets is user * password *.

L2TP Client

L2TP Client

L2TP Client Options ☒ Enable ☐ Disable

User Name

Password ☐ Unmask

Gateway (L2TP Server)

Remote Subnet

Remote Subnet Mask

MPPE Encryption

MTU (Default: 1450)

MRU (Default: 1450)

NAT ☒ Enable ☐ Disable

Require CHAP ☒ Yes ☐ No

Refuse PAP ☒ Yes ☐ No

Require Authentication ☒ Yes ☐ No

Gateway(L2TP Server): L2TP server's IP Address or DNS Name

Remote Subnet: the network of remote PPTP server

Remote Subnet Mask: subnet mask of remote PPTP server

MPPE Encryption: enable or disable Microsoft Point-to-Point Encryption

MTU: maximum transmission unit

MRU: maximum receive unit

NAT: network address translation

User Name: user name to login L2TP Server

Password: password to login L2TP Server

Require CHAP: enable or disable support chap authentication protocol

Refuse PAP: enable or disable refuse to support the pap authentication

Require Authentication: enable or disable support authentication protocol

3.1.4.3. OPENVPN

OPENVPN Server

Start Type ☐ WAN Up ☒ System

Start Type: WAN UP----start after on-line, System----start when boot up

Config via ☒ GUI ☐ Config File

Server mode ☒ Router (TUN) ☐ Bridge (TAP)

Config via: GUI----Page configuration, Config File----config File configuration

Server mode: Router (TUN)-route mode, Bridge (TAP)----bridge mode

Router (TUN):

Network
Netmask

Network: network address allowed by OPENVPN server

Netmask: netmask allowed by OPENVPN server

Bridge (TAP):

DHCP-Proxy mode ☐ Enable ☒ Disable
Pool start IP
Pool end IP
Gateway
Netmask

DHCP-Proxy mode: enable or disable DHCP-Proxy mode

Pool start IP: pool start IP of the client allowed by OPENVPN server

Pool end IP: pool end IP of the client allowed by OPENVPN server

Gateway: the gateway of the client allowed by OPENVPN server

Netmask: netmask of the client allowed by OPENVPN server

Port (Default: 1194)
Tunnel Protocol
Encryption Cipher
Hash Algorithm

Port: listen port of OPENVPN server

Tunnel Protocol: UCP or TCP of OPENVPN tunnel protocol

Encryption Cipher: Blowfish CBC, AES-128 CBC, AES-192 CBC, AES-256 CBC, AES-512 CBC

Hash Algorithm: Hash algorithm provides a method of quick access to data, including SHA1, SHA256, SHA512, MD5

Advanced Options

Advanced Options	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Use LZO Compression	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Redirect default Gateway	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Allow Client to Client	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Allow duplicate cn	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
TUN MTU Setting	<input type="text" value="1500"/> (Default: 1500)
MSS-Fix/Fragment across the tunnel	<input type="text"/> (Default: Disable)
TLS Cipher	<input type="text" value="Disable"/> ▼
Client connect script	<div><div></div></div>

Use LZO Compression: enable or disable use LZO compression for data transfer

Redirect default Gateway: enable or disable redirect default gateway

Allow Client to Client: enable or disable allow client to client

Allow duplicate cn: enable or disable allow duplicate cn

TUN MTU Setting: set the value of TUN MTU

TCP MSS: MSS of TCP data

TLS Cipher: TLS (Transport Layer Security) encryption standard supports AES-128 SHA and AES-256 SHA

Client connect script: define some client script by user self

CA Cert	<div><div></div></div>
---------	------------------------

CA Cert: CA certificate

Public Server Cert	<div><div></div></div>
--------------------	------------------------

Public Server Cert: server certificate

Private Server Key

DH PEM

Private Server Key: the key set by the server

DH PEM: PEM of the server

Additional Config

CCD-Dir DEFAULT file

TLS Auth Key

Certificate Revoke List

Additional Config: additional configurations of the server

CCD-Dir DEFAULT file: other file approaches

TLS Auth Key: authority key of Transport Layer Security

Certificate Revoke List: configure some revoke certificates

OPENVPN Client

Server IP/Name	<input type="text" value="0.0.0.0"/>	
Port	<input type="text" value="1194"/>	(Default: 1194)
Tunnel Device	<input type="text" value="TUN"/>	
Tunnel Protocol	<input type="text" value="UDP"/>	
Encryption Cipher	<input type="text" value="Blowfish CBC"/>	
Hash Algorithm	<input type="text" value="SHA1"/>	
nsCertType verification	<input type="checkbox"/>	

Server IP/Name: IP address or domain name of OPENVPN server

Port: listen port of OPENVPN client

Tunnel Device: TUN----Router mode, TAP----Bridge mode

Tunnel Protocol: UDP and TCP protocol

Encryption Cipher: Blowfish CBC, AES-128 CBC, AES-192 CBC, AES-256 CBC, AES-512 CBC

Hash Algorithm: Hash algorithm provides a method of quick access to data, including SHA1, SHA256, SHA512, MD5

nsCertType verification: support ns certificate type

Advanced Options	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Use LZO Compression	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
NAT	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Bridge TAP to br0	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Local IP Address	<input type="text"/>
TUN MTU Setting	<input type="text" value="1500"/> (Default: 1500)
MSS-Fix/Fragment across the tunnel	<input type="text"/> (Default: Disable)
TLS Cipher	<input type="text" value="Disable"/>
TLS Auth Key	<input type="text"/>
Additional Config	<input type="text"/>
Policy based Routing	<input type="text"/>

Use LZO Compression: enable or disable use LZO compression for data transfer

NAT: enable or disable NAT through function

Bridge TAP to br0: enable or disable bridge TAP to br0

Local IP Address: set IP address of local OPENVPN client

TUN MTU Setting: set MTU value of the tunnel

TCP MSS: mss of TCP data

TLS Cipher: TLS (Transport Layer Security) encryption standard supports AES-128 SHA and AES-256 SHA

TLS Auth Key: authority key of Transport Layer Security

Additional Config: additional configurations of OPENVPN server

Policy based Routing: input some defined routing policy

CA Cert

Public Client Cert

Private Client Key

CA Cert: CA certificate

Public Client Cert: client certificate

Private Client Key: client key

3.1.4.4. IPSEC

Connect Status and Control

Show IPSEC connection and status of current router on IPSEC page.

Connection status and control				
Name	Type	Common Name	status	Action
Add				

Name: the name of IPSEC connection

Type: The type and function of current IPSEC connection

Common name: local subnet, local address, opposite end address and opposite end subnet of current connection

Status: connection status: closed, negotiating, establish

Closed: this connection does not launch a connection request to opposite end

Negotiating: this connection launch a request to opposite end, is under negotiating, the connection has not been established yet

Establish: the connection has been established, enabled to use this tunnel

Action: the action of this connection, current is to delete, edit, reconnect and enable

Delete: to delete the connection, also will delete IPSEC if IPSEC has set up

Edit: to edit the configure information of this connection, reload this connection to make the configuration effect after edit

Reconnect: this action will remove current tunnel, and re-launch tunnel establish request

Enable: when the connection is enable, it will launch tunnel establish request when the system reboot or reconnect, otherwise the connection will not do it

Add: to add a new IPSEC connection

Add IPSEC connection or edit IPSEC connection

Type: to choose IPSEC mode and relevant functions in this part, supports tunnel mode client, tunnel mode server and transfer mode currently

Type	Net-to-Net Virtual Private Network
IPSEC role	<input checked="" type="radio"/> Client <input type="radio"/> Server

Connection: this part contains basic address information of the tunnel

Connection

Name	<input type="text"/>	Enabled	<input checked="" type="checkbox"/>
Local WAN Interface	vlan1 <input type="button" value="v"/>	Remote Host address	<input type="text"/>
Local Subnet	<input type="text"/>	Remote subnet	<input type="text"/>
Local Id	<input type="text"/>	Remote ID	<input type="text"/>

Name: to indicate this connection name, must be unique

Enabled: If enable, the connection will send tunnel connection request when it is reboot or re-connection, otherwise it is no need if disable

Local WAN Interface: local addresss of the tunnel

Remote Host Address: IP/domain name of end opposite; this option can not fill in if using tunnel mode server

Local Subnet: IPSec local protects subnet and subnet mask, i.e. 192.168.1.0/24; this option can not fill in if using transfer mode

Remote Subnet: IPSec opposite end protects subnet and subnet mask, i.e.192.168.7.0/24; this option can not fill in if using transfer mode

Local ID: tunnel local end identification, IP and domain name are available

Remote ID: tunnel opposite end identification, IP and domain name are available

Detection: this part contains configure information of connection detection

Detection

Enable DPD Detection ☒

Time Interval (S) Timeout (S) Action

Enable Connection Detection ☒

Enable DPD Detection: enable or disable this function, tick means enable

Time Interval: set time interval of connect detection (DPD)

Timeout: set the timeout of connect detection

Action: set the action of connect detection

Advanced Settings: this part contains relevant setting of IKE, ESP, negotiation mode, etc.

Advanced Settings

Enable advanced settings ☒

IKE Encryption IKE Integrity IKE Grouptype

IKE Lifetime hours

ESP Encryption ESP Integrity

ESP Keylife hours

☐ IKE+ESP: Use only proposed settings.

☐ IKE aggressive mode allowed. Avoid if possible (preshared key is transmitted in clear text)!

☒ Perfect Forward Secrecy (PFS)

☐ Negotiate payload compression

Enable Advanced Settings: enable to configure 1st and 2nd phase information, otherwise it

will automatic negotiation according to opposite end

IKE Encryption: IKE phased encryption mode

IKE Integrity: IKE phased integrity solution

IKE Grouptype: DH exchange algorithm

IKE Lifetime: set IKE lifetime, current unit is hour, the default is 0

ESP Encryption: ESP encryption type

ESP Integrity: ESP integrity solution

ESP Keylife: set ESP keylife, current unit is hour, the default is 0

IKE aggressive mode allowed: negotiation mode adopt aggressive mode if tick; it is main mode if non-tick

Negotiate payload compression: Tick to enable PFS, non-tick to diable PFS

Authentication: choose use share encryption option or certificate authentication option. Current is only to choose use share encryption option.

Authentication

☒ Use a Pre-Shared Key:

☐ Generate and use the X.509 certificate

3.1.4.5. GRE

GRE (Generic Routing Encapsulation) protocol is a network layer protocol (such as IP and IPX) data packets are encapsulated, so these encapsulated data packets to another network layer protocol (IP) transmission. GRE Tunnel (tunnel) technology, Layer Two Tunneling Protocol VPN (Virtual Private Network).

GRE Tunnel

GRE Tunnel ☐ Enable ☒ Disable

GRE Tunnel: enable or disable GRE function

Number	1 (fff) ▼	Delete
Status	Enable ▼	
Name	fff	
Through	PPP ▼	
Peer Wan IP Addr	120.42.46.98	
Peer Subnet	192.168.5.0/24	(eg:192.168.1.0/24)
Peer Tunnel IP	200.200.200.1	
Local Tunnel IP	200.200.200.5	
Local Netmask	255.255.255.0	

Number : Switch on/off GRE tunnel app

Status : Switch on/off someone GRE tunnel app

Name : GRE tunnel name

Through : The GRE packet transmit interface

Peer Wan IP Addr : The remote WAN address

Peer Subnet : The remote gateway local subnet, eg: 192.168.1.0/24

Peer Tunnel IP : The remote tunnel ip address

Local Tunnel IP : The local tunnel ip address

Local Netmask : Netmask of local network

Keepalive	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Retry times	<input type="text"/>
Interval	<input type="text"/>
Fail Action	Hold ▼

Keepalive : Enable or disable GRE Keepalive function

Retry times : GRE keepalive detect fail retries

Interval : The time interval of GRE keepalive packet sent

Fail Action : The action would be exec after keeping alive failed

Click on “**View GRE tunnels**” keys can view the information of GRE

GRE Tunnels list											
Number	Name	Enable	Through	Peer Wan IP Addr	Peer Subnet	Peer Tunnel IP	Local Tunnel IP	Local Netmask	Keepalive	Retry times	Fail Action
1	fff	Yes	PPP	120.42.46.98	192.168.5.0/24	200.200.200.1	200.200.200.5	255.255.255.0	No	0	Hold
<div>Refresh Close</div>											

3.1.5. Security

3.1.5.1. Firewall

You can enable or disable the firewall, filter specific Internet data types, and prevent anonymous Internet requests, ultimately enhance network security.

Firewall Protection

Firewall Protection

SPI Firewall ☒ Enable ☐ Disable

Firewall enhance network security and use SPI to check the packets into the network. To use firewall protection, choose to enable otherwise disabled. Only enable the SPI firewall, you can use other firewall functions: filtering proxy, block WAN requests, etc.

Additional Filters

Additional Filters

☐ Filter Proxy

☐ Filter Cookies

☐ Filter Java Applets

☐ Filter ActiveX

Filter Proxy: Wan proxy server may reduce the security of the gateway, Filtering Proxy will refuse any access to any wan proxy server. Click the check box to enable the function otherwise disabled.

Filter Cookies: Cookies are the website of data the data stored on your computer. When you interact with the site ,the cookies will be used. Click the check box to enable the function otherwise disabled.

Filter Java Applets: If refuse to Java, you may not be able to open web pages using the Java programming.. Click the check box to enable the function otherwise disabled.

Filter ActiveX: If refuse to ActiveX, you may not be able to open web pages using the ActiveX programming. Click the check box to enable the function otherwise disabled.

Prevent WAN Request

Block WAN Requests

- ☒ Block Anonymous WAN Requests (ping)
- ☒ Filter IDENT (Port 113)
- ☒ Block WAN SNMP access

Block Anonymous WAN Requests (ping): By selecting “Block Anonymous WAN Requests (ping)” box to enable this feature, you can prevent your network from the Ping or detection of other Internet users. so that make More difficult to break into your network. The default state of this feature is enabled ,choose to disable allow anonymous Internet requests.

Filter IDENT (Port 113): Enable this feature can prevent port 113 from being scanned from outside. Click the check box to enable the function otherwise disabled.

Block WAN SNMP access: This feature prevents the SNMP connection requests from the WAN.

After Complete the changes, click the **Save Settings** button to save your changes. Click the **Cancel Changes** button to cancel unsaved changes.

Impede WAN DoS/Bruteforce

Impede WAN DoS/Bruteforce

- ☐ Limit SSH Access
- ☐ Limit Telnet Access
- ☐ Limit PPTP Server Access
- ☐ Limit L2TP Server Access

Limit ssh Access: This feature limits the access request from the WAN by ssh, and per minute up to accept two connection requests on the same IP. Any new access request will be automatically dropped.

Limit Telnet Access: This feature limits the access request from the WAN by Telnet, and per minute up to accept two connection requests on the same IP. Any new access request will be automatically dropped.

Limit PPTP Server Access: When build a PPTP Server in the router, this feature limits the access request from the WAN by ssh, and per minute up to accept two connection requests on the same IP . Any new access request will be automatically dropped.

Limit L2TP Server Access: When build a L2TP Server in the router, this feature limits the access request from the WAN by ssh, and per minute up to accept two connection requests on the same IP. Any new access request will be automatically dropped.

Log Management

The router can keep logs of all incoming or outgoing traffic for your Internet connection.

Log

Log

☐ Enable ☒ Disable

Log: To keep activity logs, select Enable. To stop logging, select Disable. When select enable, the following page will appear.

Log

Log

☒ Enable ☐ Disable

Log Level

High

Options

Dropped

Disable

Rejected

Enable

Accepted

Enable

Log Level: Set this to the required log level. Set Log Level higher to log more actions.

Options: When select Enable, the corresponding connection will be recorded in the journal, the disabled are not recorded.

Incoming Log: To see a temporary log of the Router's most recent incoming traffic, click the Incoming Log button.

Incoming Log Table			
Source IP	Protocol	Destination Port Number	Rule
		Refresh	Close

Outgoing Log: To see a temporary log of the Router's most recent outgoing traffic, click the Outgoing Log button.

Outgoing Log Table				
LAN IP	Destination URL/IP	Protocol	Service/Port Number	Rule
192.168.1.164	223.203.188.56	TCP	www	Accepted
192.168.1.164	183.60.16.200	UDP	8000	Accepted
192.168.1.164	183.60.48.60	UDP	8000	Accepted
192.168.1.164	112.95.240.183	UDP	8000	Accepted
192.168.1.164	183.60.49.245	UDP	8000	Accepted
192.168.1.164	119.147.32.204	UDP	8000	Accepted
192.168.1.164	112.90.86.244	UDP	8000	Accepted
192.168.1.164	119.147.45.157	UDP	8000	Accepted
192.168.1.164	183.60.49.15	UDP	8000	Accepted
192.168.1.164	183.60.16.70	UDP	8000	Accepted
192.168.1.164	183.60.16.200	UDP	8000	Accepted
192.168.1.164	183.60.48.60	UDP	8000	Accepted

Click the **Save Settings** button to save your changes. Click the **Cancel Changes** button to cancel unsaved changes.

3.1.5.2. VPN Pass-through

Virtual Private Networking (VPN) is typically used for work-related networking. For VPN tunnels, the router supports OPENVPN Pass-through, PPTP Pass-through and L2TP Pass-through.

Virtual Private Network (VPN)	
VPN Passthrough	
IPSec Passthrough	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
PPTP Passthrough	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
L2TP Passthrough	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

IPSec Pass-through : Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec tunnels to pass through the router, IPSec Pass-through is enabled by default. To disable IPSec Pass-through, select Disable.

PPTP Pass-through : Point-to-Point Tunneling Protocol is the method used to enable VPN sessions to a Windows NT 4.0 or 2000 server. To allow PPTP tunnels to pass through the router, PPTP Pass-through is enabled by default. To disable PPTP Pass-through, select Disable.

L2TP Pass-through : Layer Two (2) Tunneling Protocol, an extension to the PPP protocol that enables ISPs to operate Virtual Private Networks (VPNs). L2TP merges the best features of two other tunneling protocols: PPTP from Microsoft and L2F from Cisco Systems. To allow L2TP tunnels to pass through the router, L2TP Pass-through is enabled by default. To disable L2TP Pass-through, select Disable.

Click the **Save Settings** button to save your changes. Click the **Cancel Changes** button to cancel unsaved changes.

3.1.6. Access Restrictions

3.1.6.1. WAN Access

Use access restrictions, you can block or allow specific types of Internet applications. You can set specific PC-based Internet access policies. This feature allows you to customize up to ten different Internet Access Policies for particular PCs, which are identified by their IP or MAC addresses.

Access Policy

Policy	1 ()	Delete	Summary
Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Policy Name	<input type="text"/>		
PCs	Edit List of clients		
<input type="radio"/> Deny	Internet access during selected days and hours.		
<input checked="" type="radio"/> Filter			

Two options in the default policy rules: "Filter" and "reject". If select "Deny", you will deny specific computers to access any Internet service at a particular time period. If you choose to "filter", it will block specific computers to access the specific sites at a specific time period. You can set up 10 Internet access policies filtering specific PCs access Internet services at a particular time period.

Access Policy: You may define up to 10 access policies. Click Delete to delete a policy or Summary to see a summary of the policy.

Status: Enable or disable a policy.

Policy Name: You may assign a name to your policy.

PCs: The part is used to edit client list, the strategy is only effective for the PC in the list.

Days

Everyday	Sun	Mon	Tue	Wed	Thu	Fri	Sat
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Times

24 Hours	<input checked="" type="radio"/>
From	<input type="radio"/> 00:00 To 00:00

Days: Choose the day of the week you would like your policy to be applied.

Times: Enter the time of the day you would like your policy to be applied.

Website Blocking by URL Address

Website Blocking by Keyword

Website Blocking by URL Address: You can block access to certain websites by entering their URL.

Website Blocking by Keyword: You can block access to certain website by the keywords contained in their webpage

List of clients

Enter MAC Address of the clients in this format: xx:xx:xx:xx:xx:xx

MAC 01	<input type="text" value="00:AA:BB:CC:DD:EE"/>
MAC 02	<input type="text" value="00:00:00:00:00:00"/>
MAC 03	<input type="text" value="00:00:00:00:00:00"/>
MAC 04	<input type="text" value="00:00:00:00:00:00"/>
MAC 05	<input type="text" value="00:00:00:00:00:00"/>
MAC 06	<input type="text" value="00:00:00:00:00:00"/>
MAC 07	<input type="text" value="00:00:00:00:00:00"/>
MAC 08	<input type="text" value="00:00:00:00:00:00"/>

Enter the IP Address of the clients

IP 01	192.168.1.	<input type="text" value="15"/>
IP 02	192.168.1.	<input type="text" value="0"/>
IP 03	192.168.1.	<input type="text" value="0"/>
IP 04	192.168.1.	<input type="text" value="0"/>
IP 05	192.168.1.	<input type="text" value="0"/>
IP 06	192.168.1.	<input type="text" value="0"/>

Enter the IP Range of the clients

IP Range 01	<input type="text" value="192"/>	.	<input type="text" value="168"/>	.	<input type="text" value="1"/>	.	<input type="text" value="19"/>	~	<input type="text" value="192"/>	.	<input type="text" value="168"/>	.	<input type="text" value="1"/>	.	<input type="text" value="30"/>
IP Range 02	<input type="text" value="0"/>	.	<input type="text" value="0"/>	.	<input type="text" value="0"/>	.	<input type="text" value="0"/>	~	<input type="text" value="0"/>	.	<input type="text" value="0"/>	.	<input type="text" value="0"/>	.	<input type="text" value="0"/>

set up Internet access policy

1. Select the policy number (1-10) in the drop-down menu.
2. For this policy is enabled, click the radio button next to "Enable"
3. Enter a name in the Policy Name field.
4. Click the Edit List of PCs button.
5. On the List of PCs screen, specify PCs by IP address or MAC address. Enter the appropriate IP addresses into the IP fields. If you have a range of IP addresses to filter, complete the appropriate IP Range fields. Enter the appropriate MAC addresses into the MAC fields.
6. Click the Apply button to save your changes. Click the Cancel button to cancel your unsaved changes. Click the Close button to return to the Filters screen.
7. If you want to block the listed PCs from Internet access during the designated days and time, then keep the default setting, Deny. If you want the listed PCs to have Internet filtered during the designated days and time, then click the radio button next to Filter.
8. Set the days when access will be filtered. Select every day or the appropriate days of the week.
9. Set the time when access will be filtered. Select 24 Hours, or check the box next to From and use the drop-down boxes to designate a specific time period.
10. Click the Add to Policy button to save your changes and active it.
11. To create or edit additional policies, repeat steps 1-9.
12. To delete an Internet Access Policy, select the policy number, and click the Delete button.

Note:

- 1) The default factory value of policy rules is "filtered". If the user chooses the default policy rules for "refuse", and editing strategies to save or directly to save the settings. If the strategy edited is the first, it will be automatically saved into the second, if not the first, keep the original number.
- 2) Turn off the power of the router or reboot the router can cause a temporary failure. After the failure of the router, if cannot automatically synchronized NTP time server, you need to recalibrate to ensure the correct implementation of the relevant period control function.

3.1.6.2. Packet Filter

To block some packets getting Internet access or block some Internet packets getting local network access, you can configure filter items to block these packets.

Packet Filter

Packet filter function is realized based on IP address or port of packets.

Enable Packet Filter ☒ Enable ☐ Disable

Policy Discard packets conform to the following rules ▼

Enable Packet Filter: Enable or disable “packet filter” function

Policy: The filter rule’s policy, you can choose the following options

Discard The Following--Discard packets conform to the following rules, Accept all other packets

Only Accept The Following-- Accept only the data packets conform to the following rules, Discard all other packets

Add Filter Rule

Direction OUTPUT ▼

Protocol TCP/UDP ▼

Source Ports 1 - 65535

Destination Ports 1 - 65535

Source IP 0 . 0 . 0 . 0 / 0

Destination IP 0 . 0 . 0 . 0 / 0

Add

Direction

input: packet from WAN to LAN

output: packet from LAN to WAN

Protocol: packet protocol type

Source Ports: packet's source port

Destination Ports: packet's destination port

Source IP: packet's source IP address

Destination IP: packet's destination IP address

Note: "Source Port" ,"Destination Port" ,"Source IP" ,"Destination IP" could not be all empty ,you have to input at least one of these four parameters.

3.1.7. NAT

3.1.7.1. Port Forwarding

Port Forwarding allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications.

Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. When users send this type of request to your network via the Internet, the router will forward those requests to the appropriate PC. If you want to forward a whole range of ports, see [Port Range Forwarding](#).

Forwards

Application	Protocol	Source Net	Port from	IP Address	Port to	Enable
web	TCP	192.168.8.11	8000	192.168.1.12	80	<input checked="" type="checkbox"/>
ftp	Both	192.168.8.12	24	192.168.1.12	21	<input checked="" type="checkbox"/>

Application: Enter the name of the application in the field provided.

Protocol: Chose the right protocol TCP,UDP or Both. Set this to what the application requires.

Source Net: Forward only if sender matches this ip/net (example 192.168.1.0/24).

Port from: Enter the number of the external port (the port number seen by users on the Internet).

IP Address: Enter the IP Address of the PC running the application.

Port to: Enter the number of the internal port (the port number used by the application).

Enable: Click the Enable checkbox to enable port forwarding for the application.

Check all values and click **Save Settings** to save your settings. Click the **Cancel changes** button to cancel your unsaved changes.

3.1.7.2. Port Range Forward

Port Range Forwarding allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. When users send this type of request to your network via the Internet, the router will forward those requests to the appropriate PC. If you only want to forward a single port, see [Port Forwarding](#).

Port Range Forward

Forwards

Application	Start	End	Protocol	IP Address	Enable
web-tftp	800	8100	Both	192.168.1.16	<input checked="" type="checkbox"/>
game	9000	10000	Both	192.168.1.16	<input checked="" type="checkbox"/>

[Add](#) [Remove](#)

Application: Enter the name of the application in the field provided.

Start: Enter the number of the first port of the range you want to be seen by users on the Internet and forwarded to your PC.

End: Enter the number of the last port of the range you want to be seen by users on the Internet and forwarded to your PC.

Protocol: Chose the right protocol TCP,UDP or Both. Set this to what the application requires.

IP Address: Enter the IP Address of the PC running the application.

Enable: Click the Enable checkbox to enable port forwarding for the application.

Check all values and click **Save Settings** to save your settings. Click the **Cancel changes** button to cancel your unsaved changes.

3.1.7.3. Port Triggering

Port Triggering allows you to do port forwarding without setting a fixed PC. By setting Port Triggering rules, you can allow inbound traffic to arrive at a specific LAN host, using ports different than those used for the outbound traffic. This is called port triggering since the outbound traffic triggers to which ports inbound traffic is directed.

Port Triggering

Forwards

Application	Triggered Port Range		Protocol	Forwarded Port Range		Enable
	Start	End		Start	End	
web	8000	10000	Both	20	800	<input checked="" type="checkbox"/>

[Add](#) [Remove](#)

If you want to forward ports to a PC with a static IP address, see [Port Forwarding](#) or [Port Range Forwarding](#).

Application: Enter the name of the application in the field provided.

Triggered Port Range: Enter the number of the first and the last port of the range, which should be triggered. If a PC sends outbound traffic from those ports, incoming traffic on the Forwarded Range will be forwarded to that PC.

Forwarded Port Range: Enter the number of the first and the last port of the range, which should be forwarded from the Internet to the PC, which has triggered the Triggered Range.

Enable :Click the Enable checkbox to enable port triggering for the application.

Check all values and click Save Settings to save your settings. Click the Cancel changes button to cancel your unsaved changes.

3.1.7.4. DMZ

The DMZ (DeMilitarized Zone) hosting feature allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Forwarding feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer so the Internet can see it.

Demilitarized Zone (DMZ)

DMZ

Use DMZ ☒ Enable ☐ Disable

DMZ Host IP Address 192.168.8.

Any PC whose port is being forwarded must should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

DMZ Host IP Address: To expose one PC to the Internet, select Enable and enter the computer's IP address in the DMZ Host IP Address field. To disable the DMZ, keep the default setting : Disable

Check all values and click **Save Settings** to save your settings. Click the **Cancel changes** button to cancel your unsaved changes.

3.1.8. QoS Setting

3.1.8.1. Basic

Bandwidth management prioritizes the traffic on your router. Interactive traffic

(telephony, browsing, telnet, etc.) gets priority and bulk traffic (file transfer, P2P) gets low priority. The main goal is to allow both types to live side-by side without unimportant traffic disturbing more critical things. All of this is more or less automatic. QoS allows control of the bandwidth allocation to different services, netmasks, MAC addresses and the four LAN ports.

Main WAN QoS Settings

Start QoS

☐ Enable ☒ Disable

Port

WAN

Packet Scheduler

HTB

Uplink (kbps)

0

Downlink (kbps)

0

Bkup WAN QoS Settings

Start QoS

☐ Enable ☒ Disable

Port

WAN

Packet Scheduler

HTB

Uplink (kbps)

0

Downlink (kbps)

0

Uplink (kbps) : In order to use bandwidth management (QoS) you must enter bandwidth values for your uplink. These are generally 80% to 90% of your maximum bandwidth.

Downlink (kbps) : In order to use bandwidth management (QoS) you must enter bandwidth values for your downlink. These are generally 80% to 90% of your maximum bandwidth.

3.1.8.2. Classify

Netmask Priority

Netmask Priority

Delete	IP/Mask	Priority
<input type="checkbox"/>	192.168.1.1/24	Exempt
<input type="checkbox"/>	192.168.2.3/24	Standard
<input type="checkbox"/>	192.168.3.4/32	Express
<input type="checkbox"/>	192.168.4.5/32	Bulk
<input type="button" value="Add"/>	<div>0.0.0.0 / 0</div>	

You may specify priority for all traffic from a given IP address or IP Range.

Check all values and click **Save Settings** to save your settings. Click the **Cancel changes** button to cancel your unsaved changes.

3.1.9.Applications

3.1.9.1. Serial Applications

There is a console port on the Maxon MA100-1010. Normally, this port is used to debug the router. This port can also be used as a serial port. The router has embedded a serial to TCP program. The data sent to the serial port is encapsulated by TCP/IP protocol stack and then is sent to the destination server. This function can work as a Maxon DTU (Data Terminal Unit). Please refer www.maxon.com.au for more information about this product.

Serial Applications

Serial Applications	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Baudrate	115200
Databit	8
Stopbit	1
Parity	None
Flow Control	None
Protocol	TCP(DTU)
Server Address	120.42.46.98
Server Port	55501
Device Number	12345678901
Device Id	12345678
Heartbeat Interval	60

Baudrate: The serial port's baudrate

Databit: The serial port's databit

Parity: The serial port's parity

Stopbit: The serial port's stopbit

Flow Control: The serial port's flow control type.

Enable Serial TCP Function: Enable the serial to TCP function

Protocol Type: The protocol type to transmit data.

UDP(DTU) – Data transmit with UDP protocol , work as a Maxon DTU which has application protocol and hear beat mechanism.

Pure UDP – Data transmit with standard UDP protocol.

TCP(DTU) -- Data transmit with TCP protocol , work as a Maxon DTU which has application protocol and hear beat mechanism.

Pure TCP -- Data transmit with standard TCP protocol, router is the client.

TCP Server -- Data transmit with standard TCP protocol, router is the server.

TCST -- Data transmit with TCP protocol, Using a custom data

Server Address: The data service center’s IP Address or domain name.

Server Port: The data service center’s listening port.

Device ID: The router’s identity ID.

Device Number: The router’s phone number.

Heartbeat Interval: The time interval to send heart beat packet. This item is valid only when you choose UDP(DTU) or TCP(DTU) protocol type.

TCP Server Listen Port: This item is valid when Protocol Type is “TCP Server”

Custom Heartbeat Packet : This item is valid when Protocol Type is “TCST”

Custom Registration Packets: This item is valid when Protocol Type is “TCST”

3.1.9.2. GPS Settings

Enable GPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
GPS Output Interface	<input checked="" type="checkbox"/> Net <input checked="" type="checkbox"/> Consl
Protocol	TCP ▼
GPS Center Address	0.0.0.0
GPS Center Listening Port	5001
GPS Information Update Interval	60
GPS Speed Threshold	0
Device ID	12345678 <input checked="" type="checkbox"/> Append the device ID to the tail of gps information
GPS Information Contents	<input checked="" type="checkbox"/> GPRMC <input checked="" type="checkbox"/> GPGGA <input checked="" type="checkbox"/> GPVTG <input checked="" type="checkbox"/> GPGSA <input checked="" type="checkbox"/> GPGSV <input checked="" type="checkbox"/> GPGLL

Enable GPS : Enable or disable GPS function

GPS Output Interface : This item selects the GPS output interface including network and serial port

Protocol : TCP mode or UDP mode

GPS Center Address : The GPS center’s IP Address or domain name

GPS Center Listening Port : The GPS center's listening port.

GPS Information Update Interval : The time interval between two GPS information update, unit is second

GPS Speed Threshold : The GPS speed threshold of update GPS information

Device ID : The ID of this device

Append the device ID to the tail of GPS information: Whether append the ID to the GPS information

GPS Information Contents : GPS contents selection

When GPS output interface is serial port, we should set the following serial port settings:

Baudrate	115200 ▼
Databit	8 ▼
Stopbit	1 ▼
Parity	None ▼
Flow Control	None ▼

3.1.10. Administration

3.1.10.1. Management

The Management screen allows you to change the router's settings. On this page you will find most of the configurable items of the router code.

Router Password

Router Username
Router Password
Re-enter to confirm

The new password must not exceed 32 characters in length and must not include any spaces. Enter the new password a second time to confirm it.

Note : Default username is admin.

It is strongly recommended that you change the factory default password of the router, which is admin. All users who try to access the router's web-based utility or Setup Wizard will be prompted for the router's password.

Web Access

This feature allows you to manage the router using either HTTP protocol or the HTTPS protocol. If you choose to disable this feature, a manual reboot will be required. You can also activate or not the router information web page. It's now possible to password protect this page (same username and password than above).

Web Access

Protocol	<input checked="" type="checkbox"/> HTTP <input type="checkbox"/> HTTPS
Auto-Refresh (in seconds)	<input type="text" value="3"/>
Enable Info Site	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Info Site Password Protection	<input type="checkbox"/> Enabled

Protocol : This feature allows you to manage the router using either HTTP protocol or the HTTPS protocol

Auto-Refresh : Adjusts the Web GUI automatic refresh interval. 0 disables this feature completely

Enable Info Site : Enable or disable the login system information page

Info Site Password Protection : Enable or disable the password protection feature of the system information page

Remote Access

Web GUI Management	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Use HTTPS	<input type="checkbox"/>
Web GUI Port	<input type="text" value="8080"/> (Default: 8080, Range: 1 - 65535)
SSH Management	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SSH Remote Port	<input type="text" value="22"/> (Default: 22, Range: 1 - 65535)
Telnet Management	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Remote Access : This feature allows you to manage the router from a remote location, via the Internet. To disable this feature, keep the default setting, Disable. To enable this feature, select Enable, and use the specified port (default is 8080) on your PC to remotely manage the router. You must also change the router's default password to one of your own, if you haven't already.

To remotely manage the router, enter `http://xxx.xxx.xxx.xxx:8080` (the x's represent the router's Internet IP address, and 8080 represents the specified port) in your web browser's address field. You will be asked for the router's password.

If you use https you need to specify the url as `https://xxx.xxx.xxx.xxx:8080` (not all firmwares does support this without rebuilding with SSL support).

SSH Management : You can also enable SSH to remotely access the router by Secure Shell. Note that SSH daemon needs to be enable in Services page.

Note :

If the Remote Router Access feature is enabled, anyone who knows the router's Internet IP address and password will be able to alter the router's settings.

Telnet Management : Enable or disable remote Telnet function

Cron

Cron ☒ Enable ☐ Disable

Additional Cron Jobs

Cron : The cron subsystem schedules execution of Linux commands. You'll need to use the command line or startup scripts to actually use this.

802.1x

802.1x ☒ Enable ☐ Disable

802.1x : A limited 802.1x server needed to fulfill WPA handshake requirements to allow Windows XP clients to work with WPA.

IP Filter Settings (adjust these for P2P)

TCP Congestion Control	vegas	
Maximum Ports	4096	(Default: 4096, Range: 256 - 4096)
TCP Timeout (in seconds)	3600	(Default: 3600, Range: 1 - 86400)
UDP Timeout (in seconds)	120	(Default: 120, Range: 1 - 86400)

IP Filter Settings (adjust these for P2P) : If you have any peer-to-peer (P2P) applications running on your network please increase the maximum ports and lower the TCP/UDP timeouts. This is necessary to maintain router stability because peer-to-peer applications open many connections and don't close them properly. Consider using these:

Maximum Ports: 4096

TCP Timeout: 3600 sec

UDP Timeout: 120 sec

3.1.10.2. Keep Alive

Schedule Reboot

Schedule Reboot

☒ Schedule Reboot

☒ Enable ☐ Disable

☒ Interval (in seconds)

☐ 3600

☐ At a set Time

☐ 00 : 00 Sunday

You can schedule regular reboots for the router :

Regularly after xxx seconds.

At a specific date time each week or everyday.

Note :

For date based reboots Cron must be activated. See Management for Cron activation.

3.1.10.3. Commands

Commands : You are able to run command lines directly via the Web interface.

Command Shell

Commands

Run Commands

Save Startup

Save Shutdown

Save Firewall

Save Custom Script

Run Command : You can run command lines via the web interface. Fill the text area with your command and click Run Commands to submit.

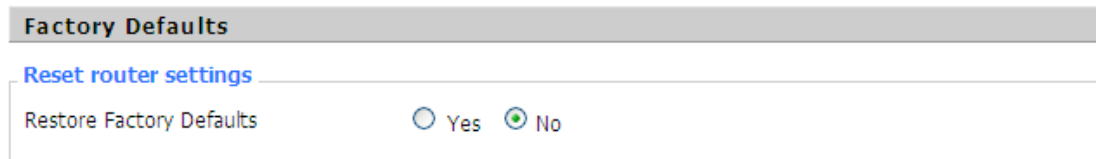
Startup : You can save some command lines to be executed at startup's router. Fill the text area with commands (only one command by row) and click Save Startup.

Shutdown : You can save some command lines to be executed at shutdown's router. Fill the text area with commands (only one command by row) and click Save Shutdown.

Firewall : Each time the firewall is started, it can run some custom iptables instructions. Fill the text area with firewall's instructions (only one command by row) and click Save Firewall.

Custom Script : Custom script is stored in /tmp/custom.sh file. You can run it manually or use cron to call it. Fill the text area with script's instructions (only one command by row) and click Save Custom Script.

3.1.10.4. Factory Defaults

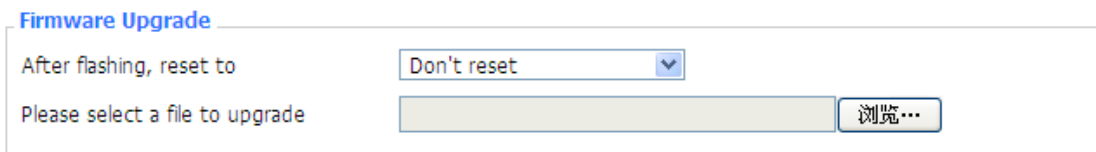


Reset router settings : Click the Yes button to reset all configuration settings to their default values. Then click the Apply Settings button.

Note :

Any settings you have saved will be lost when the default settings are restored.
After restoring the router is accessible under the default IP address 192.168.1.1 and the default password admin.

3.1.10.5. Firmware Upgrade



Firmware Upgrade : New firmware versions can be provided by Maxon. If the Router is not experiencing difficulties, then there is no need to download a more recent firmware version, unless that version has a new feature that you want to use.

Note :

When you upgrade the Router's firmware, you lose its configuration settings, so make sure you write down the Router settings before you upgrade its firmware.

To upgrade the Router's firmware:

1. Download the firmware upgrade file from the website.
2. Click the Browse... button and chose the firmware upgrade file.
3. Click the Upgrade button and wait until the upgrade is finished.

Note :

Upgrading firmware may take a few minutes.
Do not turn off the power or press the reset button!

After flashing, reset to : If you want to reset the router to the default settings for the firmware version you are upgrading to, click the Firmware Defaults option.

3.1.10.6. Backup

Backup Configuration

Backup Settings
Click the "Backup" button to download the configuration backup file to your computer.

Restore Configuration

Restore Settings
Please select a file to restore

WARNING
Only upload files backed up using this firmware and from the same model of router.
Do not upload any files that were not created by this interface!

Backup Settings : You may backup your current configuration in case you need to reset the router back to its factory default settings. Click the Backup button to back up your current configuration.

Restore Settings : Click the Browse... button to browse for a configuration file that is currently saved on your PC. Click the Restore button to overwrite all current configurations with the ones in the configuration file.

Note :

Only restore configurations with files backed up using the same firmware and the same model of router.

3.1.11. Status

3.1.11.1. Router

System

Router Name	Datamax MA100-1010
Router Model	Router
Firmware Version	v1.0 (Jun 19 2013 11:34:46) std - build 223
MAC Address	<u>00:0C:43:9C:5A:BA</u>
Host Name	
WAN Domain Name	
LAN Domain Name	
Current Time	Wed, 17 Jul 2013 06:42:56
Uptime	16:12

Router Name: name of the router, setting→basic setting to modify

Router Model: model of the router, unavailable to modify

Firmware Version: software version information

MAC Address: MAC address of WAN, setting→Clone MAC Address to modify

Host Name: host name of the router, setting→basic setting to modify

WAN Domain Name: domain name of WAN, setting→basic setting to modify

LAN Domain Name: domain name of LAN, unavailable to modify

Current Time: local time of the system

Uptime: operating uptime as long as the system is powered on

Memory

Total Available	28880 kB / 32768 kB	<div><div style="width: 88%;">88%</div></div>
Free	12436 kB / 28880 kB	<div><div style="width: 43%;">43%</div></div>
Used	16444 kB / 28880 kB	<div><div style="width: 57%;">57%</div></div>
Buffers	1660 kB / 16444 kB	<div><div style="width: 10%;">10%</div></div>
Cached	5708 kB / 16444 kB	<div><div style="width: 35%;">35%</div></div>
Active	963 kB / 16444 kB	<div><div style="width: 6%;">6%</div></div>
Inactive	1118 kB / 16444 kB	<div><div style="width: 7%;">7%</div></div>

Total Available: the room for total available of RAM (that is physical memory minus some reserve and the kernel of binary code bytes)

Free: free memory, the router will reboot if the memory is less than 500kB

Used: used memory, total available memory minus free memory

Buffers: used memory for buffers,

Cached: the memory used by high-speed cache memory

Active: active use of buffer or cache memory page file size

Inactive: not often used in a buffer or cache memory page file size

Network

IP Filter Maximum Ports 4096

Active IP Connections 43

1%

IP Filter Maximum Ports: preset is 4096, available to re-management

Active IP Connections: real time monitor active IP connections of the system, click to see the table as blow:

Active IP Connections

53

No.	Protocol	Timeout (s)	Source Address	Remote Address	Service Name	State
1	TCP	60	192.168.1.120	192.168.1.1	80	TIME_WAIT
2	TCP	30	192.168.1.120	192.168.1.1	80	TIME_WAIT
3	TCP	65	192.168.1.120	192.168.1.1	80	TIME_WAIT
4	TCP	96	192.168.1.120	192.168.1.1	80	TIME_WAIT
5	TCP	99	192.168.1.120	192.168.1.1	80	TIME_WAIT
6	TCP	70	192.168.1.120	192.168.1.1	80	TIME_WAIT
7	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
8	TCP	115	192.168.1.120	192.168.1.1	80	TIME_WAIT
9	TCP	84	192.168.1.120	192.168.1.1	80	TIME_WAIT
10	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
11	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
12	TCP	108	192.168.1.120	192.168.1.1	80	TIME_WAIT
13	TCP	3600	192.168.1.120	192.168.1.1	80	ESTABLISHED
14	TCP	93	192.168.1.120	192.168.1.1	80	TIME_WAIT
15	TCP	102	192.168.1.120	192.168.1.1	80	TIME_WAIT
16	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
17	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
18	TCP	15	192.168.1.120	192.168.1.1	80	TIME_WAIT
19	TCP	25	192.168.1.120	192.168.1.1	80	TIME_WAIT
20	TCP	90	192.168.1.120	192.168.1.1	80	TIME_WAIT
21	UDP	26	192.168.8.119	255.255.255.255	1947	UNREPLIED
22	TCP	77	192.168.1.120	192.168.1.1	80	TIME_WAIT
23	TCP	35	192.168.1.120	192.168.1.1	80	TIME_WAIT
24	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
25	TCP	40	192.168.1.120	192.168.1.1	80	TIME_WAIT
26	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
27	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
28	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
29	TCP	4	192.168.1.120	192.168.1.1	80	TIME_WAIT
30	UDP	31	192.168.8.160	224.0.0.1	9166	UNREPLIED
31	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT

Active IP Connections: total active IP connections

Protocol: connection protocol

Timeouts: connection timeouts, unit is second

Source Address: source IP address

Remote Address: remote IP address

Service Name: connecting service port

Status: displayed status

3.1.11.2. WAN

Connection Type	Automatic Configuration - DHCP
Connection Uptime	Not available

Connection Type: disabled, static IP, automatic configuration-DHCP, PPPOE, PPTP, L2TP, 3G/UMTS

Connection Uptime: connecting uptime; If disconnect, display Not available

IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
DNS 1	
DNS 2	
DNS 3	

IP Address: IP address of router WAN

Subnet Mask: subnet mask of router WAN

Gateway: the gateway of router WAN

DNS1, DNS2, DNS3: DNS1/DNS2/DNS3 of router WAN

Remaining Lease Time	0 days 23:38:43
	<input type="button" value="DHCP Release"/> <input type="button" value="DHCP Renew"/>

Remaining Lease Time: remaining lease time of IP address in DHCP way

DHCP Release: release DHCP address


DHCP Renew: renew IP address in DHCP way, default is 1 day

Login Status	Disconnected <input type="button" value="Connect"/>
--------------	---

Login Status: connection status of WAN

Disconnection: disconnect

Connection: connect

Module Type	WCDMA/HSDPA-I(820W) MODULE
	
Signal Status	-67 dBm
Network	WCDMA

Module Type: module type in 3G/UMTS way

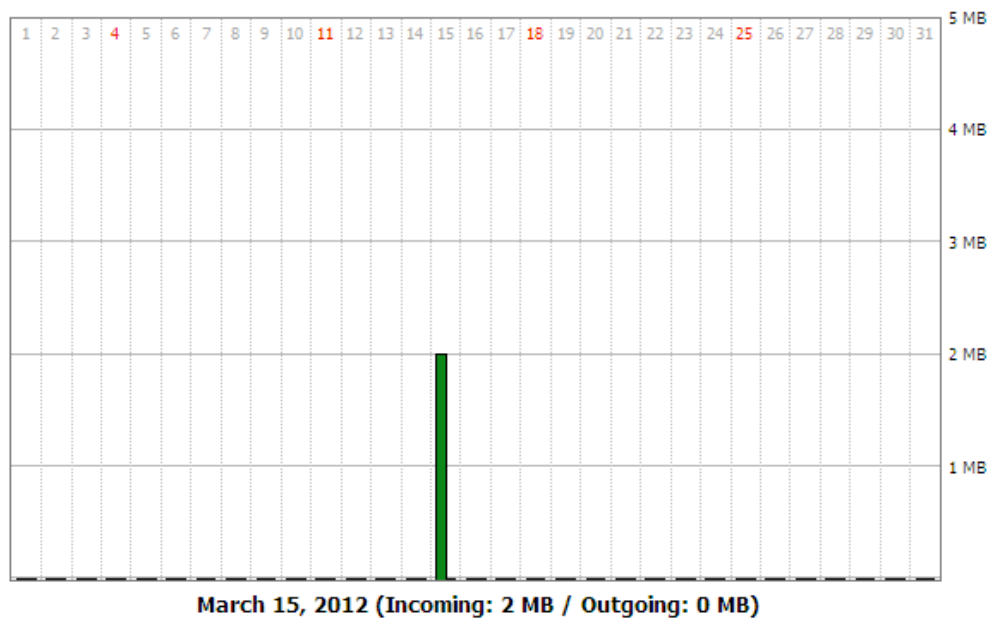
Signal Status: signal intensity of the module in 3G/UMTS way

Network: network type of the module in 3G/UMTS way

Total Traffic

Incoming (MBytes)	0
Outgoing (MBytes)	0

Traffic by Month



Previous Month

Next Month

Total Flow: flow from power-off last time until now statistics, download and upload direction

Monthly Flow: the flow of a month, unit is MB

Last Month: the flow of last month

Next Month: the flow of next month

Data Administration

Backup Restore Delete

Backup: backup data administration

Restore: restore data administration

Delete: delete data administration

3.1.11.3. LAN

LAN Status

MAC Address	<u>00:0C:43:30:52:77</u>
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
Local DNS	0.0.0.0

MAC Address: MAC Address of the LAN port Ethernet

IP Address: IP Address of the LAN port

Subnet Mask: Subnet Mask of the LAN port

Gateway: Gateway of the LAN port

Local DNS: DNS of the LAN port

Active Clients

Host Name	IP Address	MAC Address	Conn. Count	Ratio [4096]
*	192.168.1.120	<u>10:78:D2:98:C9:46</u>	57	1%

Host Name: host name of LAN client

IP Address: IP address of the client

MAC Address: MAC address of the client

Conn. Count: connection count caused by the client

Ratio: the ratio of 4096 connection

Dynamic Host Configuration Protocol

DHCP Status

DHCP Server	Enabled
DHCP Daemon	uDHCpD
Start IP Address	192.168.1.100
End IP Address	192.168.1.149
Client Lease Time	1440 minutes

DNCP Server: enable or disable the router work as a DHCP server




DHCP Daemon: the agreement allocated using DHCP including DNSMasq and uDHCpD

Starting IP Address: the starting IP Address of the DHCP server's Address pool

Ending IP Address: the ending IP Address of the DHCP server's Address pool

Client Lease Time: the lease time of DHCP client

DHCP Clients

Host Name	IP Address	MAC Address	Client Lease Time	Delete
PC-201011161332	192.168.1.142	00:21:5C:33:4D:29	1 day 00:00:00	
jack-lincw	192.168.1.117	44:37:E6:3F:45:54	1 day 00:00:00	
*	192.168.1.149	00:0C:E7:00:00:00	1 day 00:00:00	

Host Name: host name of LAN client

IP Address: IP address of the client

MAC Address: MAC address of the client

Expires: the expiry the client rents the IP address

Delete: click to delete DHCP client

Connected PPPOE Clients

Interface	User Name	Local IP	Delete
ppp0	hometest	192.168.10.10	

Interface: the interface assigned by dial-up system

User Name: user name of PPPoE client

Local IP: IP address assigned by PPPoE client

Delete: click to delete PPPoE client

Connected L2TP Server

Interface	Local IP	Remote IP	Delete
ppp0	172.168.8.2	172.168.8.1	

Interface: the interface assigned by dial-up system

Local IP: tunnel IP address of local L2TP

Remote IP: tunnel IP address of L2TP server

Delete: click to disconnect L2TP

Connected L2TP Clients

Interface	User Name	Local IP	Remote IP	Delete
ppp1	hometest	192.168.50.2	120.42.46.98	

Interface: the interface assigned by dial-up system

User Name: user name of the client

Local IP: tunnel IP address of L2TP client

Remote IP: IP address of L2TP client

Delete: click to delete L2TP client

Connected PPTP Server

Interface	Local IP	Remote IP	Delete
ppp0	172.168.8.2	172.168.8.1	

Interface: the interface assigned by dial-up system

Local IP: tunnel IP address of local PPTP

Remote IP: tunnel IP address of PPTP server

Delete: click to disconnect PPTP

Connected PPTP Clients

Interface	User Name	Local IP	Remote IP	Delete
ppp1	hometest	192.168.5.1	120.42.46.98	

Interface: the interface assigned by dial-up system

User Name: user name of the client

Local IP: tunnel IP address of PPTP client

Remote IP: IP address of PPTP client

Delete: click to delete PPTP client

3.1.11.4. Wireless

Wireless Status

MAC Address	<u>00:0C:43:9C:5A:BB</u>
Radio	Radio is On
Mode	AP
Network	Mixed
SSID	ssid
Channel	6 (2437 MHz)
TX Power	71 mW
Rate	72 Mb/s
Encryption - Interface wl0	Disabled
PPTP Status	Disconnected

MAC Address: MAC address of wireless client

Radio: display whether radio is on or not

Mode: wireless mode

Network: wireless network mode

SSID: wireless network name

Channel: wireless network channel

TX Power: reflection power of wireless network

Rate: reflection rate of wireless network

Encryption-Interface wlo: enable or disable Encryption-Interface wlo

PPTP Status: show wireless pptp status

Wireless Packet Info

Received (RX)	91125 OK, no error	100%
Transmitted (TX)	11957 OK, no error	100%

Received (RX): received data packet

Transmitted (TX): transmitted data packet

Wireless Nodes

Clients

MAC Address	Interface	Uptime	TX Rate	RX Rate	Signal	Noise	SNR	Signal Quality
- None -								

MAC Address: MAC address of wireless client

Interface: interface of wireless client

Uptime: connecting uptime of wireless client

TX Rate: transmit rate of wireless client

RX Rate: receive rate of wireless client

Signal: the signal of wireless client

Noise: the noise of wireless client

SNR: the signal to noise ratio of wireless client

Signal Quality: signal quality of wireless client

Neighbor's Wireless Networks

SSID	Mode	MAC Address	Channel	Rssi	Noise	beacon	Open	dtim	Rate	Join Site
MAXONAUSTRALIA	AP	b0:48:7a:a0:5b:a0	6	-100	-95	0	No	0	300(b/g/n)	Join
linksys	AP	c8:d7:19:ba:4a:90	11	-86	-95	0	No	0	300(b/g/n)	Join

[Refresh](#)

[Close](#)

Neighbor's Wireless Network: display other networks nearby

SSID: the name of wireless network nearby

Mode: operating mode of wireless network nearby

MAC Address: MAC address of the wireless nearby

Channel: the channel of the wireless nearby

Rssi: signal intensity of the wireless nearby

Noise: the noise of the wireless nearby

Beacon: signal beacon of the wireless nearby

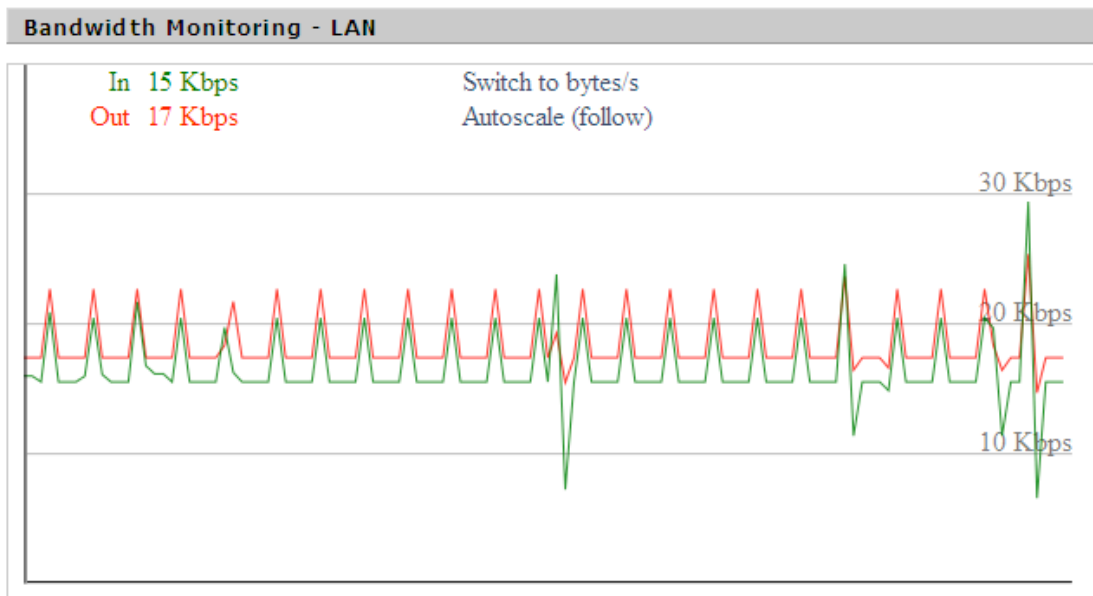
Open: the wireless nearby is open or not

Dtim: delivery traffic indication message of the wireless nearby

Rate: speed rate of the wireless nearby

Join Site: click to join wireless network nearby

3.1.11.5. Bandwidth

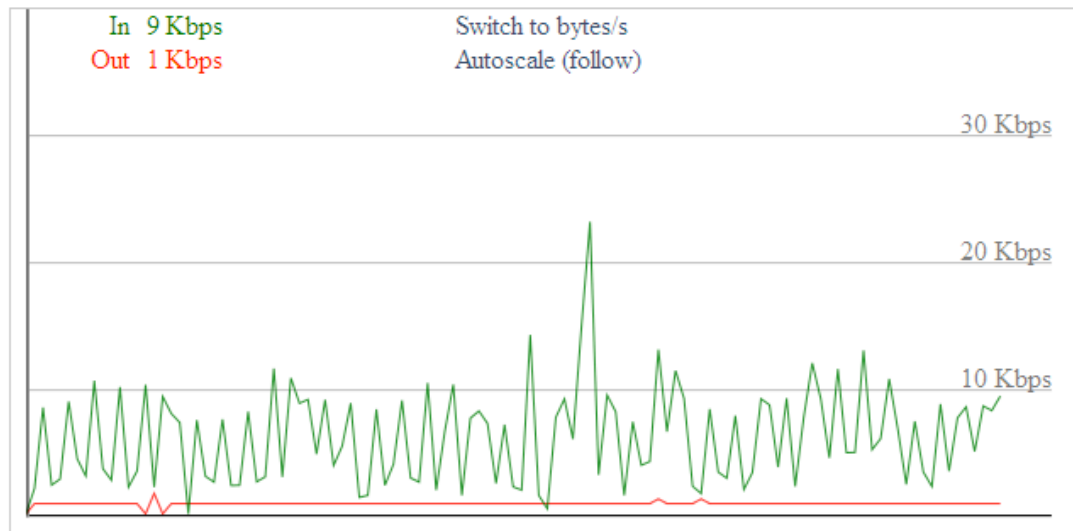


Bandwidth Monitoring-LAN Graph

abscissa axis: time

vertical axis: speed rate

Bandwidth Monitoring - WAN

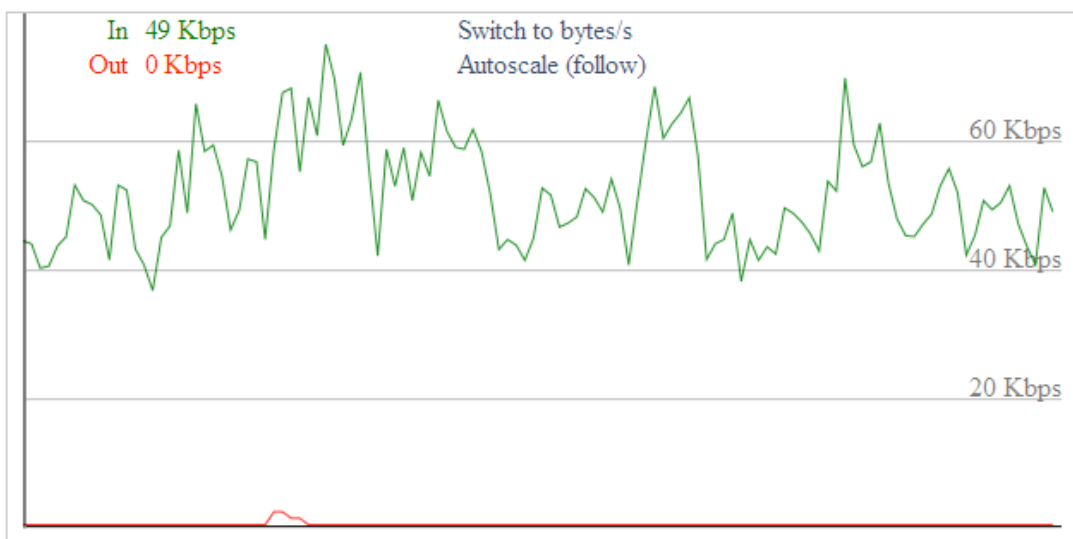


Bandwidth Monitoring-WAN Graph

abscissa axis: time

vertical axis: speed rate

Bandwidth Monitoring - Wireless (wl0)



Bandwidth Monitoring-Wireless (W10) Graph

abscissa axis: time

vertical axis: speed rate

3.1.11.6. Sys-Info

Router

Router Name	Datamax MA100-1010
Router Model	Router
LAN MAC	<u>00:0C:43:9C:5A:B9</u>
WAN MAC	<u>00:0C:43:9C:5A:BA</u>
Wireless MAC	<u>00:0C:43:9C:5A:BB</u>
WAN IP	123.209.7.114
LAN IP	192.168.1.1

Router Name: the name of the router

Router Model: the model of the router

LAN MAC: MAC address of LAN port

WAN MAC: MAC address of WAN port

Wireless MAC: MAC address of the wireless

WAN IP: IP address of WAN port

LAN IP: IP address of LAN port

Wireless

Radio	Radio is On
Mode	AP
Network	Mixed
SSID	ssid
Channel	6 (2437 MHz)
TX Power	71 mW
Rate	72 Mb/s

Radio: display whether radio is on or not

Mode: wireless mode

Network: wireless network mode

SSID: wireless network name

Channel: wireless network channel

TX Power: reflection power of wireless network

Rate: reflection rate of wireless network

Wireless Packet Info

Received (RX)	6982 OK, no error
Transmitted (TX)	1498 OK, no error

Received (RX): received data packet

Transmitted (TX): transmitted data packet

Wireless

Clients

MAC Address	Interface	Uptime	TX Rate	RX Rate	Signal	Noise	SNR	Signal Quality
- None -								

MAC Address: MAC address of wireless client

Interface: interface of wireless client

Uptime: connecting uptime of wireless client

TX Rate: transmit rate of wireless client

RX Rate: receive rate of wireless client

Signal: the signal of wireless client

Noise: the noise of wireless client

SNR: the signal to noise ratio of wireless client

Signal Quality: signal quality of wireless client

Services

DHCP Server	Enabled
ff-radauth	Disabled
USB Support	Disabled

DHCP Server: enabled or disabled

ff-radauth: enabled or disabled

USB Support: enabled or disabled

Memory

Total Available	28.2 MB / 32.0 MB
Free	11.2 MB / 28.2 MB
Used	17.0 MB / 28.2 MB
Buffers	1.8 MB / 17.0 MB
Cached	6.3 MB / 17.0 MB
Active	1.5 MB / 17.0 MB
Inactive	0.8 MB / 17.0 MB

Total Available: the room for total available of RAM (that is physical memory minus some reserve and the kernel of binary code bytes)

Free: free memory, the router will reboot if the memory is less than 500kB

Used: used memory, total available memory minus free memory

Buffers: used memory for buffers, total available memory minus allocated memory

Cached: the memory used by high-speed cache memory

Active: Active use of buffer or cache memory page file size

Inactive: Not often used in a buffer or cache memory page file size

DHCP

DHCP Clients

Host Name	IP Address	MAC Address	Expires
*	192.168.1.143	xx:xx:xx:xx:DD:45	1 day 00:00:00
four-488e1df5fa	192.168.1.125	xx:xx:xx:xx:D8:F7	1 day 00:00:00
Mycenae-PC	192.168.1.116	xx:xx:xx:xx:5E:30	1 day 00:00:00

Host Name: host name of LAN client

IP Address: IP address of the client

MAC Address: MAC address of the client

Expires: the expiry the client rents the IP address

4. Chapter 4 Appendix

The following steps describe how to setup Windows XP Hyper Terminal.

1. Press "Start" → "Programs" → "Accessories" → "Communications" → "Hyper Terminal"



2. Input connection name, choose "OK"
3. Choose the correct COM port which connects to modem, choose "OK"



4. Configure the serial port parameters as following, choose “OK”

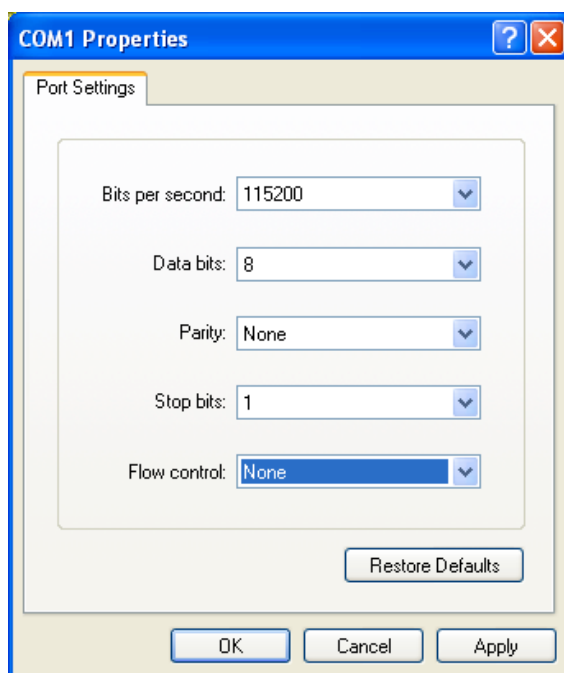
Bits per second: 115200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None



5. Complete Hyper Terminal operation, It runs as following

